IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In Re: BPS DIRECT LLC, AND CAEBELA'S LLC, WIRETAPPING LITIGATION	MDL NO. 3074 E.D. Ps. Action Nos.: 23-md-3074 22-cv-4709 23-cv-2282 23-cv-2287 23-cv-2293 23-cv-2294 23-cv-2295 23-cv-2306 23-cv-2338

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Brian Calvert, Heather Cornell, Timothy Durham, Marilyn Hernandez, Greg Moore, Peter Montecalvo, Arlie Tucker, and Brittany Vonbergen (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, hereby file this consolidated class action complaint against Defendants BPS Direct, LLC, d/b/a Bass Pro Shops ("BPS") and Cabela's LLC ("Cabela's") (collectively, "Defendants"), and in support thereof allege the following:

INTRODUCTION

1. This is a class action brought against Defendants for the wiretapping of electronic communications of visitors to Defendants' websites, www.basspro.com and www.cabelas.com ("Defendants' Websites"), and all of Defendants' Websites' subpages. Defendants procure third-party vendors, such as Microsoft Corporation ("Microsoft"), Quantum Metric, and Mouseflow to embed snippets of JavaScript computer code ("Session Replay Code") on Defendants' Websites, which then deploys on each website visitor's internet browser for the purpose of intercepting and recording the website visitor's electronic communications with Defendants' Websites (*i.e.*,

computer to computer data communications), including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box, both intentional and unintentional), URLs of web pages visited, and/or other electronic communications in real-time (collectively, "Website Communications"). The Session Replay Code procured by Defendants surreptitiously and instantaneously intercepted, stored, and recorded everything Plaintiffs and the Class Members did on Defendants' Websites, *e.g.*, what they searched for, what they looked at, the information they inputted, and what they clicked on for the entire duration of their visit.

2. These third-party vendors, such as Microsoft, Quantum Metric, Mouseflow, and others (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Defendants' request, and capture and store the Website Communications of each website visitor.

3. After intercepting and capturing the Website Communications, Defendants' and the Session Replay Providers can use those Website Communications to recreate website visitors' entire visit to Defendants' Websites. The Session Replay Providers can create, using the swaths of website users' data they collect from users' browsing sessions and browsing devices, a video replay of the user's behavior on the websites and provide it to BPS or Cabela's, respectively, for analysis. Defendants' procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to Defendants' Websites for the entire duration of their interaction with the websites.

4. Defendants knowingly, willfully, and intentionally procured the interception of, and used, the electronic communications at issue without the knowledge or prior consent of Plaintiffs or the Class Members. Defendants did so for their own financial gain and in violation of Plaintiffs' and the Class Members' substantive legal privacy rights under the various wiretapping laws and other state statutes and the common law.

5. The Session Replay Code utilized by Defendants is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that allows Session Replay Providers to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to Defendants' Websites.

6. The CEO of a major Session Replay Provider – while discussing the merger of his company with another Session Replay Provider – publicly exposed why companies like Defendants employ the use of Session Replay Code on their websites: "The combination of Clicktale and Contentsquare heralds an unprecedented goldmine of digital data that enables companies to interpret and predict the impact of any digital element -- including user experience, content, price, reviews and product -- on visitor behavior[.]"[1] This CEO further admitted that "this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50 martech partners. With a global community of customers and partners, we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences."[2]

7. Unlike typical website analytics services that provide simple aggregate statistics, the Session Replay Code utilized by Defendants is intended to record and playback individual browsing sessions. The technology also permits companies like Defendants to view the interactions of visitors on their websites in real-time, including capturing partial text field submissions that users did not intend to send to Defendants' (for example, by closing the browser

[1] *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed Aug. 14, 2023).

[2] *Id.*

before hitting “submit”), and certainly did not intend to send to third-party Session Replay Providers.

8. Defendants’ conduct violates the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, California Penal Code § 631, Statutory Larceny, Cal. Pen. Code §§ 484, 496, Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Maryland Wiretapping and Electronic Surveillance Act, Md. Code. Ann (“MWESA”)., Cts. & Jud. Proc. § 10-401, Massachusetts Wiretapping Statute, Mass. Gen. Laws ch. 272 §99(Q), Missouri Wiretap Act, Mo. Ann. Stat. § 542.400, *et seq.*, Pennsylvania Wiretap and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. §§ 5701, *et seq*. (“WESCA”), and constitutes an invasion of privacy rights of website visitors under each relevant state’s law.

9. Plaintiffs bring this action individually and on behalf of a nationwide class of all natural persons in the United States and in its territories whose Website Communications were intercepted through the use of Session Replay Code embedded on Defendants’ Websites (the “Nationwide Class”). Plaintiffs also bring this action on behalf of all natural persons in the states of California, Maryland, Massachusetts, Missouri, and Pennsylvania whose Website Communications were intercepted through the use of Session Replay Code embedded on Defendants’ Websites (the “State Subclasses,” and, collectively with the Nationwide Class, the “Class”). Plaintiffs seek all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, declaratory and injunctive relief, and attorneys’ fees and costs.

PARTIES

10. Plaintiff Brian Calvert is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Lawrence County, Pennsylvania. Plaintiff Calvert accessed www.cabelas.com while in Pennsylvania.

11. Plaintiff Heather Cornell is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Forest County, Pennsylvania. Plaintiff Cornell accessed www.basspro.com while in Pennsylvania.

12. Plaintiff Timothy Durham is a citizen of the State of California, and at all times relevant to this action resided and was domiciled in Los Angeles County, California. Plaintiff Durham accessed www.cabelas.com while in California.

13. Plaintiff Marilyn Hernandez is a citizen of the State of Mayland, and at all times relevant to this action, resided and was domiciled in Prince George’s County, Maryland. Plaintiff Hernandez accessed www.basspro.com while in Maryland.

14. Plaintiff Peter Montecalvo is a citizen of the State of Connecticut, and at all times relevant to this action resided and was domiciled in Middlesex County, Connecticut. Plaintiff Montecalvo accessed www.cabelas.com while in Massachusetts.

15. Plaintiff Greg Moore is a citizen of the State of California, and at all times relevant to this action resided and was domiciled in San Diego County, California. Plaintiff Moore accessed www.basspro.com while in California.

16. Plaintiff Arlie Tucker is a citizen of the State of Missouri, and at all times relevant to this action, resided and was domiciled in Franklin County, Missouri. Plaintiff Tucker accessed www.basspro.com and www.cabelas.com while in Missouri.

17. Plaintiff Brittany Vonbergen is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action resided and was domiciled in Delaware County, Pennsylvania. Plaintiff Vonbergen accessed www.basspro.com while in Pennsylvania.

18. Defendant BPS is a limited liability company organized under the laws of Delaware, and its principal place of business is in Springfield, Missouri. BPS Direct, LLC is wholly owned by Bass Pro, LLC.[3] Bass Pro, LLC is a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri.[4] The sole member of Bass Pro, LLC is Huntsman Holdings, LLC, a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. The members of Huntsman Holdings, LLC are Bass Pro Group, LLC and ASHCo, Inc. Bass Pro Group, LLC is a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. ASHCo, Inc., is a corporation organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. The sole member of Bass Pro Group, LLC is Bass Pro Holdings, LLC, a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. Bass Pro Holdings, LLC's sole member is Johnny Morris Outdoors, LLC, a multi-member LLC, with three members. The three members of Johnny Morris Outdoors, LLC are American Sportsman Holdings Co., Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC. American Sportsman Holdings Co. is a corporation organized under the laws of the State of

[3] *State Of Delaware, Ex Rel. Kathleen Jennings, Attorney General Of The State Of Delaware, v. Cabela's Inc., et al.*, Case No. 1:23-cv-00790-RGA at ECF No. 3 (Respondents' Corporate Disclosure Statement) (July 24, 2023).

[4] *See* ECF No. 47 at 3 (stipulated facts).

Missouri with its principal place of business in Missouri. Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC are investment companies that provided funding for the Bass Pro acquisition of Cabela's. The members of these two LLCs are unknown to any person employed by any of the Bass Pro and TMBC, LLC entities or TMBC, LLC's parent entities.[5] Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC are limited liability companies organized under the laws of the State of Delaware. Upon information and belief, Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC each have individual members that are residents of the State of Pennsylvania. Defendant BPS is, thus, a citizen of Missouri and Pennsylvania – and possibly other states.

19. Defendant Cabela's is a single member limited liability company organized under the laws of Delaware with its principal place of business in Springfield, Missouri. Cabela's LLC is wholly owned by Bass Pro, LLC, which is wholly owned by Huntsman Holdings, LLC. Huntsman Holdings, LLC is an indirect, wholly-owned subsidiary of American Sportsman Holdings Co., a Missouri corporation with its principal place of business at 2500 E. Kearney St., Springfield, Missouri.

20. The members of Huntsman Holdings, LLC are Bass Pro Group, LLC and ASHCo, Inc. Bass Pro Group, LLC is a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. ASHCo, Inc., is a corporation organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. *Id.* The sole member of Bass Pro Group, LLC is Bass Pro Holdings, LLC, a single-member limited liability company organized under the laws of the State of Delaware with its principal place of business in Springfield, Missouri. Bass Pro Holdings,

[5] *See id.* (as to Bass Pro); *see also Hafer v. TMBC, LLC d/b/a Cabela's*, *et al.*, Case No. 5:20-cv-06371, ECF No. 7 (Defendants TMBC LLC, LLC and Cabela's Wholesale, LLC Disclosure Statement Form as to TMBC, LLC and its parent entities).

LLC's sole member is Johnny Morris Outdoors, LLC, a multi-member LLC, with three members. The three members of Johnny Morris Outdoors, LLC are American Sportsman Holdings Co., Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC. American Sportsman Holdings Co. is a corporation organized under the laws of the State of Missouri with its principal place of business in Missouri. *Id.* Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC are investment companies that provided funding for the Bass Pro acquisition of Cabela's. The members of these two LLCs are unknown to any person employed by any of the Bass Pro and TMBC, LLC entities or TMBC, LLC's parent entities. Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC are limited liability companies organized under the laws of the State of Delaware. Upon information and belief, Outdoor Holdings, LLC and WSCP VII Mockingjay II, LLC each have individual members that are residents of the State of Pennsylvania.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendants.

22. This Court has general jurisdiction over BPS pursuant to Pa. C.S.A. § 5301. Specifically, this Court has general jurisdiction over BPS because BPS is an out-of-state business association registered to do business under the laws of the Commonwealth of Pennsylvania since June 16, 2010. As part of registering to do business in the Commonwealth of Pennsylvania, BPS "shall enjoy the same rights and privileges as a domestic entity and shall be subject to the same liabilities, restrictions, duties and penalties . . . imposed on domestic entities." Pa. C.S.A. § 402(d).

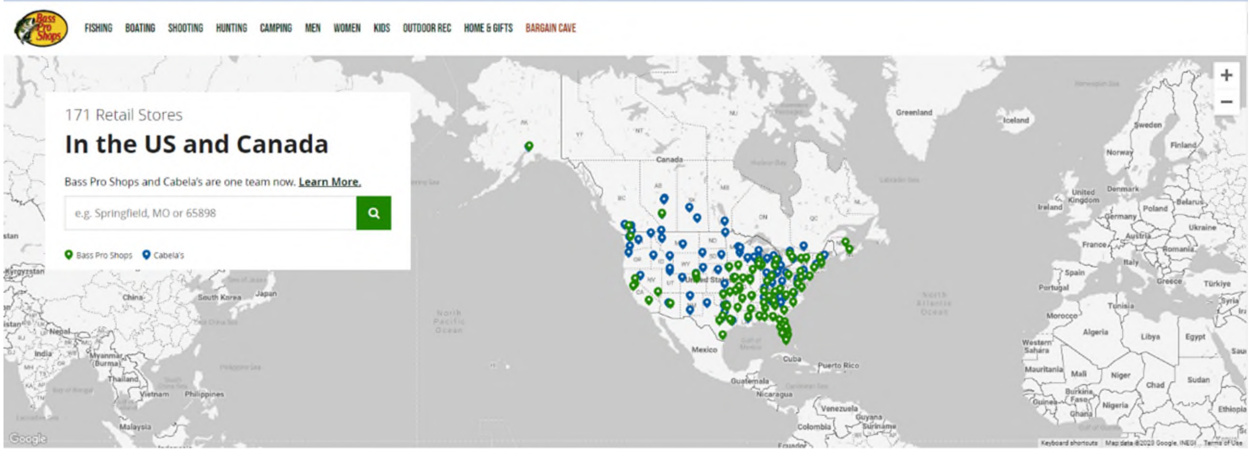
Among other things, Pennsylvania law is explicit that "qualification as a foreign entity under the laws of [the] Commonwealth" shall permit state courts to "exercise general personal jurisdiction" over a registered foreign partnership, limited partnership, partnership association, profession association, unincorporate association and other similar entities, just as they can over domestic entities. Pa. C.S.A. § 5301. Thus, by registering to do business in the Commonwealth of Pennsylvania and benefiting from the opportunity to do business in the Commonwealth Pennsylvania, BPS has consented to being subject to general jurisdiction in the Commonwealth of Pennsylvania.

23. In the alternative, this Court has specific personal jurisdiction over Defendants because a substantial part of the events and conduct giving rise to Plaintiffs' claims and harm occurred in the Commonwealths of Pennsylvania and Massachusetts, and the States of California, Maryland, and Missouri, and throughout the United States. The privacy violations complained of herein resulted from Defendants' purposeful and tortious acts directed towards citizens throughout the United States. At all relevant times, Defendants knew that their practices would directly result in the collection of information from individuals located within each state of the United States, including but not limited to, California, Maryland, Massachusetts, Missouri, and Pennsylvania while those individuals browsed Defendants' Websites. Defendants chose to avail themselves of the business opportunities of marketing, selling and shipping their goods in each state in the United States and specifically in California, Maryland, Massachusetts, Missouri, and Pennsylvania, and procuring the interception of real-time data from website visitors' sessions initiated by individuals while located in those places, and the claims alleged herein arise from those activities.

24. Defendants also knew that many users visit and interact with Defendants' Websites while they are physically present in the United States, and its territories.

25. Both desktop and mobile versions of Defendants' Websites allow a user to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Defendants are continuously made aware that their websites are being visited by people located in the United States and its territories, and that such website visitors are being wiretapped in violation of the federal Wiretap Act, and other state statutes and common laws.

26. Defendants have a physical presence throughout the United States, maintaining one or more brick and mortar stores located in Pennsylvania (1 Bass Pro Shops; 1 Cabela's); California (4 Bass Pro Shops); Missouri (6 Bass Pro Shops; 1 Cabela's; 1 Bass Pro Catalogue Outlet); Massachusetts (1 Bass Pro Shops; 1 Cabela's); Maryland (1 Bass Pro Shops), among other physical sites as reflected in the below map.[6]



171 Retail Stores

In the US and Canada

Bass Pro Shops and Cabela's are one team now. **Learn More.**

27. In addition to the physical retail stores identified above, Defendants have a "robust e-commerce" presence. In particular, Bass Pro and Cabela's each ship products to the 50 States

[6] *See* https://stores.basspro.com/ (identifying 171 Retail Stores for both Bass Pro and Cabela's); *see also* **Exhibit A (**identifying each and every Bass Pro Shops and Cabela's located in the United States).

and Territories through Defendants' Websites to respective website visitors whose privacy has been violated as a result of Defendants' purposeful actions towards those States and Territories.[7]

28. Additionally, Bass Pro and Cabela's each provide website visitors with the ability to check on their respective websites whether a product is in stock at a particular brick and mortar location. Going a step further, while procuring third parties to track their customers online, Bass Pro and Cabela's each give the website visitors the ability to order products on the website for "In Store Pick Up" at one of the 171 physical retail locations around the United States.

29. Defendants' digital presence targets specific locations with targeted ads specific to the community in which the ad is placed. In fact, according to a Bass Pro Case Study, Joe Gies, Senior Marketing Manager of Creative and Photography Services (at Bass Pro) provides with respect to its "robust e-commerce" that:

> We try very hard to create a one-to-one dialog and presentation to our customers, no matter where they may live or shop," says Joe Gies, Sr. Marketing Manager of Creative and Photography Services (at Bass Pro). [...] "Digital editions are also uploaded to each store website. These are produced every two weeks and have driven significant sales volume nationwide. Their effectiveness is due in large part to their deliberately customized [sic] regional and demographic appeal. While other retailers typically customize [sic] inserts by price, Bass Pro also customises [sic] each version according to actual customer interests." "You've got a fisherman in South Florida who's fishing for large-mouth bass," Gies says. "He'll be using a specific type of plug or lure—like an orange-colored worm. But we don't want to feature those types of lures to a fisherman in Wisconsin or Michigan who's fishing for northern pike. To have authenticity in our presentation, we always feature products that are relevant to each geography **-** just as we hire people in our stores that have local knowledge and expertise.[8]

30. This Court has personal jurisdiction over Defendants because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from each of the 50 States,

[7] *See* **Exhibit B** (Shipping Details, Providing for Shipping to the 50 States and Territories).

[8] *See* Making Personal Connections, COMOSOFT (2018), *available at* https://www.comosoft.eu/case-study-bass-pro-shops/ (last accessed Aug. 14, 2023).

including California, Maryland, Massachusetts, Missouri, and Pennsylvania. Defendants procured and embedded Session Replay Code, which it used to allow Session Replay Providers to collect data directly from website visitors in each of the 50 States, violating federal and statutory law as well as common law.

31. Furthermore, Defendants actively use the data collected by Session Replay Providers in all 50 States to specifically target citizens of each state with marketing and advertising content which results in an increased profit to Defendants at a significant cost to Plaintiffs and Class Members in the form of privacy.

32. Defendants' decision to place or procure the placement of Session Reply Code to collect the data of nationwide residents of the United States, including Pennsylvania, Missouri, Maryland, Massachusetts, and California, is by deliberate and intentional design.

33. Though Plaintiffs and Class Members do not currently have the ability to do so, if a user chose not to grant Defendants' permission to collect the user data or employ the Session Replay Code on their computers and/or mobile devices, Defendants' profits would be reduced because they would not be able to track Plaintiffs, gather information about them, or push ads which result in profit to Bass Pro and Cabela's.

34. Defendants' deliberate gathering of the data is intentionally targeted toward citizens, residents, and visitors of each state, including Plaintiffs and the Class, and constitutes purposeful activity directed at individuals and their browsing devices in each of the 50 states, including but not limited to Missouri, Pennsylvania, Maryland, Massachusetts, and California.

35. Defendants' deliberate placement of Session Replay Code on the computers and mobile devices of unwitting browsers in the United States results in a trespass to chattels – i.e., the computers and/or mobile devices and/or the data contained therein; a conversion of chattels – i.e.,

the computers and/or mobile devices and/or the data contained therein. Given the placement of the Session Replay Code on Defendants' Websites to intercept data from website browsers nationwide, and the use of such intercepted data for specific targeting advertisements and profit, Defendants could not be surprised to be hailed into Pennsylvania, Missouri, Maryland, Massachusetts, California, or any other State or Territory.

36. Additionally, Defendants derive substantial revenue from online purchases of visitors whose Website Communications are being intercepted. Upon information and belief, Defendants generate revenue from thousands of individuals who make purchases of products online throughout the 50 States (given its shipping policies), including in this District. By deriving revenue from consumers in the 50 States, this constitutes purposeful activity directed at individuals and their browsing devices in each of the 50 States. Defendants regularly promote and advertise their products in all 50 states.

37. Pursuant to 28 U.S.C. §1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

ARTICLE III STANDING

38. Plaintiffs all have Article III standing to pursue their claims. As an initial matter, the statutory claims pleaded by Plaintiffs below codify substantive rights to privacy. *See e.g., In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020) ("[T]he legislative history and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA."); *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117–18 (9th Cir. 2019) ("[T]he intrusion itself makes defendant subject to liability…wiretapping is actionable…a wiretapping plaintiff need not allege any further harm to have standing.").

39. Plaintiffs' claims arise under the core substantive provisions of the Federal Wiretapping Statute, Computer Fraud and Abuse Act, State Wiretapping statutes, and State privacy, theft, trespass to chattels, conversion to chattels, and unfair competition statutes, and as such, confer standing.

40. The core provisions of the statutes pled below are targeted at the substantive intrusion that occurs when private communications are intercepted by someone who does not have the right to access them, rather than merely setting out a procedure for handling data.

41. Importantly, the Federal Wiretapping Statute and its analogous state counterparts are content-neutral laws of general applicability, whose primary purpose is to protect the privacy of wire, oral, and electronic communications by virtue of the fact that they were illegally intercepted i.e., "by virtue of the source rather than the subject matter." *Bartnicki v. Vopper*, 532 U.S. 514, 517 (2001).

42. In the counts pleaded herein, Plaintiffs plead statutes that codify a content-specific extension of the substantive right to privacy: these statutes protect Plaintiffs' substantive privacy interest in their Website Communications. Every interception and disclosure of Plaintiffs' Website Communications offends the interests that these statutes protect and constitutes a concrete injury.

43. Plaintiffs allege that Defendants procured Session Replay Providers to collect their data without consent and have violated the concrete privacy interests that the Federal Wiretapping Statute, Computer Fraud and Abuse Act, State Wiretapping statutes, and State privacy, theft, and unfair competition statutes, as well as the common law torts of invasion of privacy and intrusion upon seclusion, protect.

44. Moreover, Plaintiffs allege that Defendants' procurement of Session Replay Providers to surreptitiously and instantaneously record every Website Communication is highly offensive and Plaintiffs have suffered concrete injury from Defendants' conduct.

45. Plaintiffs allege specific facts demonstrating that the only reason Defendants have access to the aggregated data of Plaintiffs and Class Members is through the illegal collection and storage of information from Plaintiffs' Website Communications by third parties without consent. These allegations constitute concrete injuries under the substantive rights the statutes – and the common law torts - protect.

46. That the information collected by third parties procured by Defendants was private Website Communications and was later used by Defendants, and by third parties, to facilitate their own products and services for financial gains also constitutes a concrete injury to Plaintiffs and Class Members.

47. Plaintiffs also allege that the third parties procured by Defendants aggregate and store their data under unique identifiers. Thus, even if the individual data points gathered are anonymous by themselves, when aggregated, Session Replay Providers and Defendants use them to uniquely identify each user, creating a "fingerprint" for each individual, which supports a showing of concrete harm.

48. Defendants have profited from Plaintiffs' Website Communications and have profited from the collection of Plaintiffs' data. All class members seek individual damages for these concrete injuries.

49. Plaintiffs also allege that their Website Communications have monetary value for which they were not paid. Because statutes pleaded by Plaintiffs (UCL, for example) afford them the right to prevent Defendants and their Session Replay Providers from utilizing their data for

profit, they have a property interest in their data and have suffered an injury-in-fact by Defendants' collection, storage, use and sharing of Plaintiffs' private browsing information.

50. In addition, Plaintiffs have Article III standing to pursue injunctive relief. To establish standing for prospective injunctive relief, a plaintiff must demonstrate "continuing, present adverse effects." *City of Los Angeles v. Lyons,* 461 U.S. 95, 102 (1983).

51. Plaintiffs desire to continue to use Defendants' Websites but Defendants' conduct is ongoing; Defendants continue to unlawfully cause the interception of the Website Communications of Plaintiffs and Class Members any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Defendants' conduct has not stopped, and they will continue to allow third parties to collect users' private browsing data for their own use without Plaintiffs' and Class Members' express consent.

52. Plaintiffs have pled sufficient facts alleging concrete injuries for common law torts of invasion of privacy and intrusion upon seclusion, the Federal Wiretapping Statute, Computer Fraud and Abuse Act, State Wiretapping statutes, and State privacy, theft and unfair competition statutes.

<u>FACTUAL ALLEGATIONS</u>

A. Website User and Usage Data Have Immense Economic Value

53. The "world's most valuable resource is no longer oil, but data."[9]

54. Last year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*,

[9] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), *available at* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last accessed Aug. 14, 2023).

customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[10] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[11]

55. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[12]

56. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[13] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[14]

57. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [*i.e.*, $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license

[10] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY (Aug. 5, 2022; updated Aug. 25, 2022), *available at* https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last accessed Aug. 14, 2023).

[11] *Id.*

[12] Brad Brown, Kumar Kanagasabai, Prashant Pant & Gonçalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), *available at* https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data (last accessed Aug. 14, 2023).

[13] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), *available at* https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf (last accessed Aug. 14, 2023).

[14] *Id.* at 25.

number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military are estimated to cost USD 55."[15]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Defendants' Websites

58. Consumers are skeptical and wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[16]

59. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website hosts and not be shared with a third-party they know nothing about.[17] As such, website visitors reasonably expect that their interactions with a website should not be released to third-parties unless explicitly stated.[18]

60. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

61. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

[15] *Id.*

[16] Lance Whitney, *Data privacy is a growing concern for more consumers*, TECHREPUBLIC (Aug. 17, 2021), *available at* https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/ (last accessed Aug. 14, 2023).

[17] *CUJO AI Recent Survey Reveals U.S. Internet Users' Expectations and Concerns Towards Privacy and Online Tracking*, CUJO AI (May 26, 2020), *available at* https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html (last accessed Aug. 14, 2023).

[18] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[19]

62. Moreover, according to a study by Pew Research Center, a significant majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[20]

63. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software – which asks users for clear, affirmative consent before allowing companies to track users – 85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[21]

C. How Session Replay Code Works

64. Session Replay Code, such as that implemented on Defendants' Websites, enables website operators to intercept, capture, read, observe, re-route, forward, redirect, record, save, analyze and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with detailed insights into the user behavior

[19] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), *available at* https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last accessed Aug. 14, 2023).

[20] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019), *available at* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed Aug. 14, 2023).

[21] Margaret Taylor, *How Apple screwed Facebook*, WIRED, (May 19, 2021), *available at* https://www.wired.co.uk/article/apple-ios14-facebook (last accessed Aug. 14, 2023).

by intercepting and recording website visitors "as they click, scroll, type or navigate across different web pages."[22]

65. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, has enabled private browsing such as "Incognito Mode" with the intention of masking their activities and information, or has not finished submitting the data to the website operator.[23] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[24]

66. The Session Replay Code utilized by Defendants works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of communications initiated by the actions the user takes.[25] Simply

[22] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), *available at* https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/ (last accessed Aug. 14, 2023).

[23] *Id.*

[24] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), *available at* https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0 (last accessed Aug. 14, 2023).

[25] These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. A POST request is used to send data to a server. *See, e.g., HTTP Request Methods, available at* https://www.w3schools.com/tags/ref_httpmethods.asp (last accessed Aug. 14, 2023).

put, when a user interacts with the website, they transmit substantive information via electronic communications in the form of instructions to Defendants' computer servers utilized to operate the website. These commands are sent as messages instructing the website host, like Defendants, what content was being viewed, clicked on, requested and/or inputted by the user.

67. When Defendants' Websites deliver Session Replay Code to a user's browser, the user's browser will follow the code's instructions by contemporaneously sending duplicated responsive messages of the user's communications, in the form of "Event" data, to a designated third-party Session Replay Provider server. Upon information and belief, the servers receiving the event data is exclusively controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

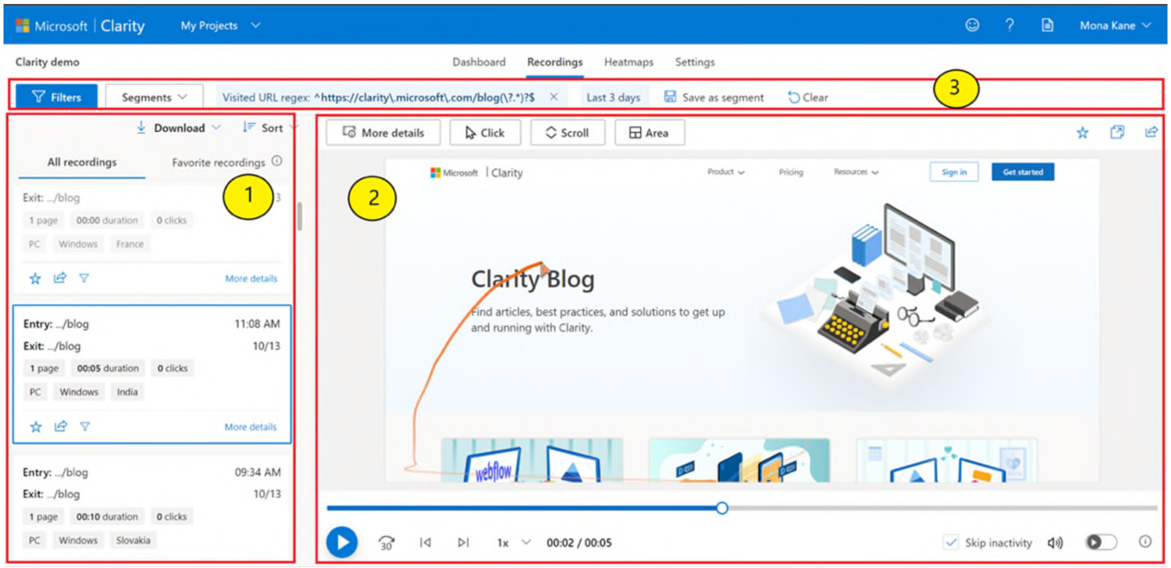
68. The types of communications captured by the Session Replay Code utilized by Defendants encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entries, and numerous other forms of a user's navigation and interaction through Defendants' Websites. To permit a reconstruction of a user's visit accurately, the Session Replay Code is capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

69. Unless specifically masked through configurations chosen by the website owner, visible contents of Website Communications are also transmitted to the Session Replay Provider. Upon information and belief, Defendants do not utilize any masking configuration settings available to them and thereby transmit all the captured data to their Session Replay Providers.

70. Once the events from a user session have been recorded by a Session Replay Code, Defendants' procured Session Replay Providers store the raw data to be interpreted and reproduced so that Defendants can view a visual reenactment of the user's visit through the Session Replay Provider's proprietary service platform, usually in the form of a video, meaning that "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[26] Moreover, the raw event data is neither readily accessible or interpretable by Defendants themselves, instead it is in the custody and control of the Session Replay provider, who has the ability to interpret and replay the data.

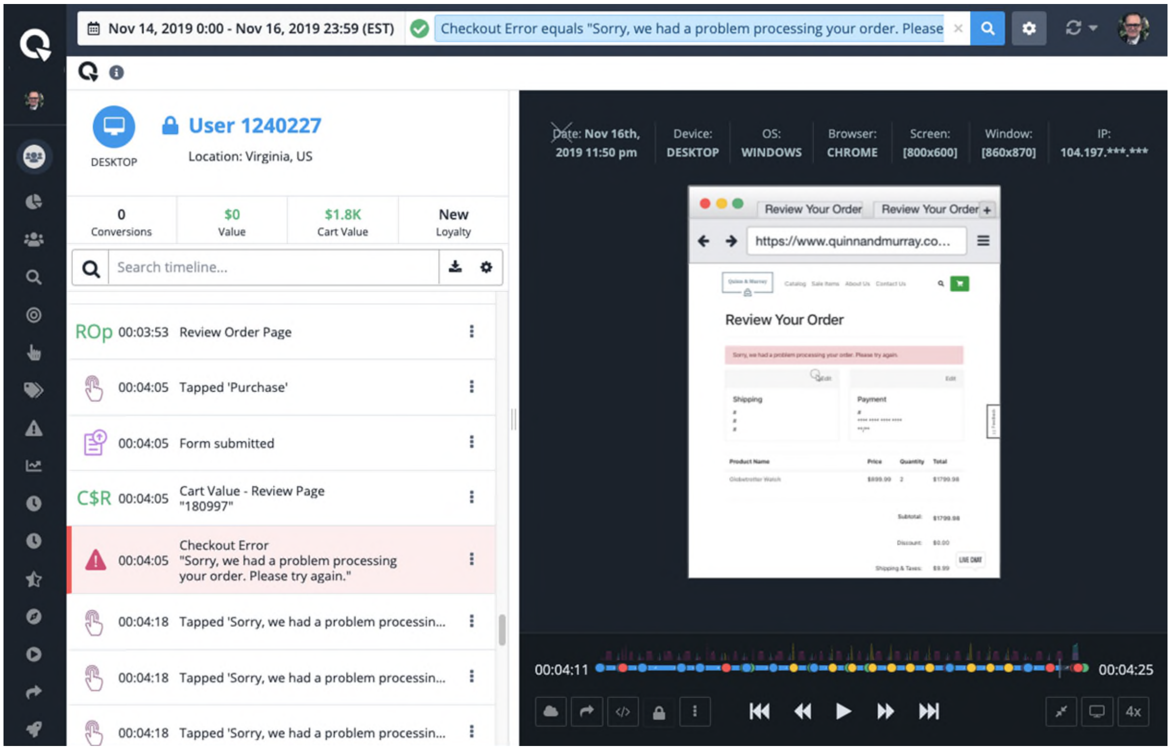
71. The following screenshots provide an example of a typical recording of a visit to a website captured utilizing the Session Replay Codes embedded by Defendants, which include mouse movements, keystrokes and clicks, search terms, content viewed, and personal information inputted by the website visitor:

CLARITY



[26] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), *available at* https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/ (last accessed Aug. 14, 2023).

QUANTUM METRIC



Checkout Error equals "Sorry, we had a problem processing your order. Please

User 1240227

Location: Virginia, US

0	$0	$1.8K	New
Conversions	Value	Cart Value	Loyalty

ROp 00:03:53 Review Order Page

00:04:05 Tapped 'Purchase'

00:04:05 Form submitted

C$R 00:04:05 Cart Value - Review Page "180997"

00:04:05 Checkout Error "Sorry, we had a problem processing your order. Please try again."

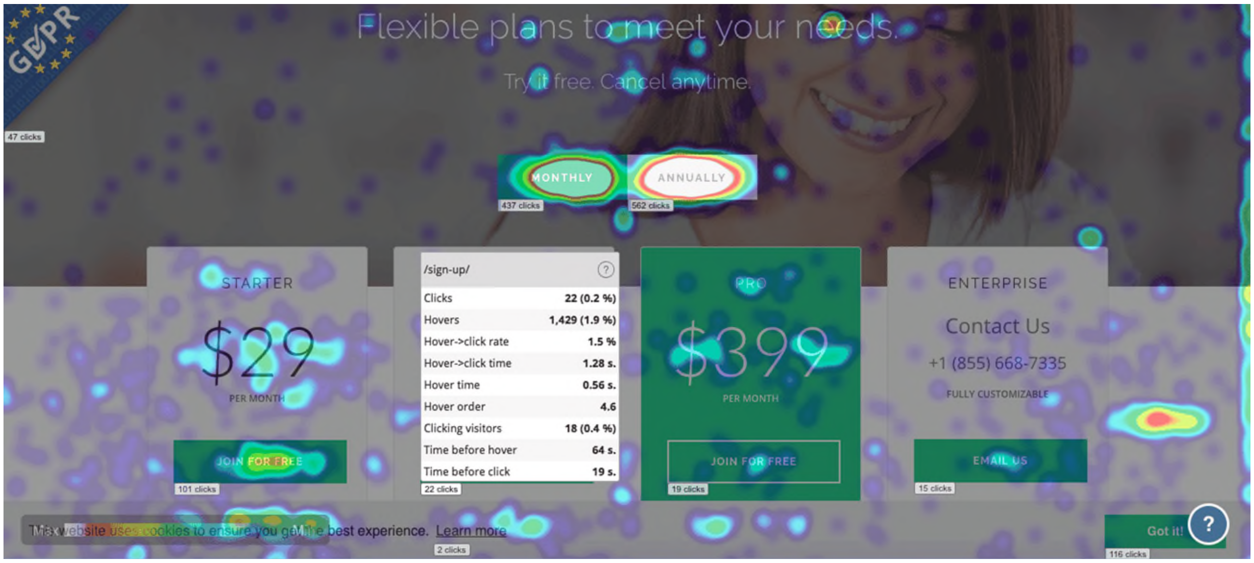
00:04:18 Tapped 'Sorry, we had a problem processin...

00:04:18 Tapped 'Sorry, we had a problem processin...

00:04:18 Tapped 'Sorry, we had a problem processin...

Date:	Device:	OS:	Browser:	Screen:	Window:	IP:
Nov 16th, 2019 11:50 pm	DESKTOP	WINDOWS	CHROME	[800x600]	[860x870]	104.197.***.***

MOUSEFLOW



/sign-up/	
Clicks	22 (0.2 %)
Hovers	1,429 (1.9 %)
Hover->click rate	1.5 %
Hover->click time	1.28 s.
Hover time	0.56 s.
Hover order	4.6
Clicking visitors	18 (0.4 %)
Time before hover	64 s.
Time before click	19 s.

72. The extent and detail of the data collected by the Session Replay Providers for users of the technology, such as Defendants, far exceeds the stated purpose and Plaintiffs' and the Class Members' reasonable expectations when visiting websites like those of Defendant. Indeed, in a

patent dispute, a highly utilized Session Replay Provider openly admitted that this type of technology is utilized by companies like Defendants to make a profit: "[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale)."[27]

73. Further, because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages. Upon information and belief, the Session Replay Code utilized by Defendants captures data including such highly sensitive information.

74. Most alarming, the Session Replay Code captures data that the user did not even intentionally transmit to a website during a visit, and then makes that data available to Defendants when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code will nevertheless cause the non-submitted text to be sent to the designated event-response-receiving Session Replay Provider's server before the user deletes the text or leaves the page. This information will then be viewable to Defendants when accessing the session replay through the Session Replay Provider.

75. Session Replay Code does not necessarily anonymize user sessions, either.

[27] *Content Square SAS v. Quantum Metric, Inc.*, Case No. 1:20-cv-00832-LPS, Compl. ¶ 8 [DE 1] (D. Del. Jun. 22, 2020).

76. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

77. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

78. Third, some Session Replay Providers, including those utilized by Defendants, explicitly offer website owners functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[28]

79. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

80. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

[28] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited August 8, 2023); *FAQ - Are you able to follow user sessions across devices?*, Quantum Metric, https://www.quantummetric.com/faq/ (last visited August 8, 2023); *How does Mouseflow detect new and returning visitors?*, Mouseflow, https://help.mouseflow.com/en/articles/4361083-how-does-mouseflow-detect-new-and-returning-visitors (last visited August 8, 2023).

81. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[29] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [… .] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[30] Moreover, users are deprived of their capacity to consent to the additional storage of their communications and personal information by a third-party.

82. The privacy concerns arising from Session Replay Code are not theoretical or imagined. The CEO and founder of LOKKER, a provider of data privacy and compliance solutions has said "[consumers] should be concerned" about the use of Session Replay Code because "they won't know these tools are operating 'behind the scenes' of their site visit" and "even if the company disclosed that they are using these tools, consumers wouldn't likely be able to opt-out and still use the site."[31] True to this statement, Defendants' Websites offer no opportunity to opt-out of its use of Session Replay Code, including if a user utilizes a private browsing mode on their browser.

[29] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

[30] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[31] Mark Huffner, *Is 'session replay software' a privacy threat or just improving your web experience*, Consumer Affairs (Oct. 25, 2022), https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html.

83. Indeed, the news is replete with examples of the dangers of Session Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about his analyses of popular apps, found that Air Canada's iPhone app wasn't properly masking the session replays they were sent, exposing unencrypted credit card data and password information.[32] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[33]

84. Further, multiple companies have removed Session Replay Code from their websites after it was discovered the Session Replay Code captured highly sensitive information. For instance, in 2017, Walgreens stopped sharing data with a Session Replay Provider after it was discovered that the Session Replay Provider gained access to website visitors' sensitive information.[34] Indeed, despite Walgreens' extensive use of manual redactions for displayed and inputted data, the Session Replay Provider still gained access to full names of website visitors, their medical conditions, and their prescriptions.[35]

85. Following the Walgreens incident, Bonobos, a men's clothing retailer, announced that it was eliminating data sharing with a Session Replay Provider after it was discovered that the Session Replay Provider captured credit card details, including the cardholder's name and billing address, and the card's number, expiration, and security code from the Bonobos' website.[36]

[32] Zach Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without Asking*, TechCrunch (Feb. 6, 2019), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.

[33] *Id.*

[34] Nitasha Tiku, *The Dark Side of 'Replay Sessions' That Record Your Every Move Online*, WIRED (Nov. 16, 2017), https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/.

[35] Englehardt, *supra* note 26.

[36] Tiku, *supra* note 34.

86. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[37] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[38]

87. Consistent with Apple's concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including the following examples:

(a) ***The Dark Side of 'Replay Sessions' That Record Your Every Move Online***, located at https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/ (last visited August 8, 2023);

(b) ***Session-Replay Scripts Disrupt Online Privacy in a Big Way***, located at https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/ (last visited August 8, 2023);

(c) ***Are Session Recording Tools a Risk to Internet Privacy?***, located at https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/ (last visited August 8, 2023);

[37] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[38] *Id.*

(d) ***Session Replay is a Major Threat to Privacy on the Web***, located at https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720 (last visited August 8, 2023);

(e) ***Session Replay Scripts Could be Leaking Sensitive Data***, located at https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161 (last visited August 8, 2023);

(f) ***Website Owners can Monitor Your Every Scroll and Click***, located at https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html (last visited August 8, 2023); and

(g) ***Sites Using Session Replay Scripts Leak Sensitive User Data***, located at https://www.helpnetsecurity.com/2017/11/20/session-replay-data-leak (last visited August 8, 2023).

D. Defendants Secretly Wiretap and Procure Session Replay Providers to Wiretap their website visitors' Electronic Communications

88. Defendants BPS and Cabela's own, manage, and/or operate the websites www.basspro.com and www.cabelas.com, respectively. Defendants are online and brick-and-mortar retailers for outdoor products, such as hunting gear and apparel, and camping equipment.

89. However, unbeknownst to the millions of individuals perusing Defendants' products online, Defendants intentionally procure and embed Session Replay Code from Session Replay Providers, such as Microsoft, Quantum Metric, and Mouseflow, on www.basspro.com and www.cabelas.com to track and analyze websites user communications with Defendants' Websites.

90. Each of these Session Replay Codes used by Defendants provide detailed information about website user sessions, interactions, and engagement, with the capacity to break down users by device type, location, and other dimensions.[39]

91. As such, the Session Replay providers collected and continue to collect Plaintiffs' and Class Members' highly personal information and substantive communications that can be tied directly to a website user's identity as it monitors, records, and collects a website user's every move.

92. In order for Session Replay Code to capture website visitors' interactions with a website, the Session Replay Provider's JavaScript must be installed on the website, either directly hard-coded on the website or via a third-party platform, such as Google Tag Manager.[40] Microsoft Clarity, Quantum Metric, and Mouseflow are embedded in Defendants' Websites by adding the relevant JavaScript code into the HyperText Markup Language (HTML) underlying Defendants' Websites. As with all HTML code, Session Replay Code is not visible to a user who is navigating a webpage through a standard browser's default view because by design a browser will interpret HTML, without showing it, in order to render a more user-friendly display that is the designer's intended presentation of the website to a visitor.

93. The Session Replay Code on Defendants' Websites can be revealed to technical users who understand web technologies and can enable alternative display modes that will show underlying HTML, such as "developer tools," but even then, the users would first need to know

[39] *See* Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity, (last visited Sep. 8, 2022); *Search for Recordings by a User's IP Address, Location, and Other Identifiers*, Mouseflow, https://help.mouseflow.com/en/articles/5882714-search-for-recordings-by-a-user-s-ip-address-location-and-other-identifiers (last visited August 8, 2023); *see also supra* note 28.

[40] *Set Up Clarity*, Microsoft (Jul. 18, 2022), https://docs.microsoft.com/en-us/clarity/clarity-setup.

what they are looking for to find the script. Developer tools are intended for website programmers, and are generally not meaningful or comprehensible by those without a background in computer science.

94. Once Session Replay JavaScript was installed on Defendants' Websites, Microsoft, Quantum Metric, and Mouseflow began collecting website user's interactions, sometimes in as little as within two hours of installation.[41] Once properly installed and functional, the wiretapping commences immediately on the visitor's web browser when the visitor loads a website in their browser.

95. Data collected by Session Replay Providers is then stored in the respective provider's servers and/or cloud service, where the provider retains access to that information in order to provide the session replay services through its platform.[42]

96. Defendants' procurement and use of Session Replay Codes through various Session Replay Providers to collect Plaintiffs' and Class Members' Website Communications, constitutes wiretapping in violation of numerous states' statutes and common law..

E. Plaintiffs' and Class Members' Experiences

Plaintiff Calvert

97. While in Pennsylvania, Plaintiff Calvert visited www.cabelas.com and certain of its subpages on his computer. He browsed for different products for sale and communicated with Cabela's website by using his mouse to hover and click on certain products and typing search words into the search bar.

[41] *Frequently Asked Questions*, Microsoft, https://docs.microsoft.com/en-us/clarity/faq, (last visited Aug. 24, 2022).

[42] *Id.*

98. Even though Plaintiff Calvert did not end up purchasing any products on his visits to Cabela's website, the Session Replay Code nevertheless instantaneously captured his Website Communications throughout his visits. Indeed, through Cabela's procurement of Session Replay Code, Plaintiff Calvert's Website Communications were automatically and secretly intercepted by using Cabela's website.

99. During Plaintiff Calvert's visit to Cabela's website, Plaintiff Calvert, through his computer, transmitted electronic communications in the form of instructions to Cabela's computer servers utilized to operate the website. The commands were sent as messages instructing Cabela's what content was being viewed, clicked on, requested and/or inputted by Plaintiff Calvert. The communications sent by Plaintiff Calvert to Cabela's servers included, but were not limited to, the following actions taken by Plaintiff Calvert while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff Calvert, pages and content viewed by Plaintiff Calvert, scroll movement, and copy and paste actions.

100. Cabela's responded to Plaintiff Calvert's electronic communications by supplying—through its website—the information requested by Plaintiff Calvert.

101. Plaintiff Calvert reasonably expected that his visit to Cabela's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as he browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Calvert that his visit to the website was being recorded by Cabela's through a third party.

102. Defendants' data collection is highly offensive and Plaintiff Calvert has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Calvert's personal browsing histories without consent.

Plaintiff Cornell

103. While in Pennsylvania, Plaintiff Cornell visited www.basspro.com and certain of its subpages on her computer in July 2022. She browsed for different products for sale and communicated with BPS's website by using her mouse to hover and click on certain products and type search words into the search bar.

104. During Plaintiff Cornell's visit, she ultimately purchased a Bass Pro Shops Eclipse Mesh-Back Canopy Chair in Cloisonne Blue. During this transaction, Plaintiff Cornell communicated with BPS by, *inter alia*, telling BPS what product she was interested in, what color chair she wanted, and where she wanted the chair shipped (i.e., her address and other personal information). In return, BPS communicated with Plaintiff Cornell by informing Plaintiff Cornell of the price of the product and requesting other information, including asking Plaintiff Cornell to provide certain information, including her name, address, and payment information. Plaintiff Cornell provided this information to BPS by using her keyboard to enter her name, address, and payment and billing information into form fields during the checkout process.

105. During Plaintiff Cornell's visit to BPS's website, Plaintiff Cornell, through her computer, transmitted electronic communications in the form of instructions to BPS's computer servers utilized to operate the website. The commands were sent as messages instructing BPS what content was being viewed, clicked on, requested and/or inputted by Plaintiff Cornell. The communications sent by Plaintiff Cornell to BPS's servers included, but were not limited to, the following actions taken by Plaintiff Cornell while on the website: mouse clicks and movements,

keystrokes, search terms, substantive information inputted by Plaintiff Cornell, pages and content viewed by Plaintiff Cornell, scroll movement, and copy and paste actions.

106. BPS responded to Plaintiff Cornell's electronic communications by supplying—through its website—the information requested by Plaintiff Cornell.

107. Plaintiff Cornell reasonably expected that her visit to BPS's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as she browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Cornell that her visit to the website was being recorded by BPS through a third party.

108. Defendants' data collection is highly offensive and Plaintiff Cornell has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Cornell's personal browsing histories without consent.

Plaintiff Hernandez

109. While in Maryland, Plaintiff Hernandez visited www.basspro.com and certain of its subpages on her computer in March 2022. She browsed for jackets for sale and communicated with BPS's website by using her mouse to hover and click on certain products and typing search words into the search bar.

110. Even though Plaintiff Hernandez did not end up purchasing any products on her to BPS's website, the Session Replay Code nevertheless instantaneously captured her Website Communications throughout her visit. Indeed, through BPS's procurement of Session Replay Code, Plaintiff Hernandez's Website Communications were automatically and secretly intercepted by using BPS's website.

111. During Plaintiff Hernandez's visit to BPS's website, Plaintiff Hernandez, through her computer, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff Hernandez. The communications sent by Plaintiff Hernandez to BPS's servers included, but were not limited to, the following actions taken by Plaintiff Hernandez while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff Hernandez, pages and content viewed by Plaintiff Hernandez, scroll movement, and copy and paste actions.

112. BPS responded to Plaintiff Hernandez's electronic communications by supplying—through its website—the information requested by Plaintiff Hernandez.

113. Plaintiff Hernandez reasonably expected that her visit to BPS's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as she browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Hernandez that her visit to the website was being recorded by Cabela's through a third party.

114. Defendants' data collection is highly offensive and Plaintiff Hernandez has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Hernandez's personal browsing histories without consent.

Plaintiff Montecalvo

115. While in Massachusetts, Plaintiff Montecalvo visited www.cabelas.com on his computer, smartphone, and iPad to search for hunting and fishing gear.

116. Plaintiff Montecalvo has consistently visited Cabela's Websites between 2010 and through 2021. Specifically, since 2019, Plaintiff Montecalvo visited Cabela's website on his laptop, smart phone, and iPad, approximately one to three times each year while in Massachusetts.

117. During some of Plaintiff Montecalvo's visits, he made multiple purchases, including for a RedHead Last Chance Light Duty Belt. During this transaction in particular, Plaintiff Montecalvo communicated with Cabela's by, *inter alia*, telling Cabela's what product he was interested in, what color belt he wanted, and where he wanted the belt shipped (i.e., his address and other personal information). In return, Cabela's communicated with Plaintiff Montecalvo by informing Plaintiff Montecalvo of the price of the product and requesting other information, including asking Plaintiff Montecalvo to provide certain information, including his name, address, and payment information. Plaintiff Montecalvo provided this information to Cabela's by using his keyboard to enter his name, address, and payment and billing information into form fields during the checkout process.

118. During Plaintiff Montecalvo's visits to Cabela's website, Plaintiff Montecalvo, through his computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff Montecalvo. The communications sent by Plaintiff Montecalvo to Cabela's servers included, but were not limited to, the following actions taken by Plaintiff Montecalvo while on the website: mouse clicks and movements, keystrokes, search terms,

substantive information inputted by Plaintiff Montecalvo, pages and content viewed by Plaintiff Montecalvo, scroll movement, and copy and paste actions.

119. Cabela's responded to Plaintiff Montecalvo's electronic communications by supplying—through its website—the information requested by Plaintiff Montecalvo.

120. Plaintiff Montecalvo reasonably expected that his visit to Cabela's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as he browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Montecalvo that his visit to the website was being recorded by Cabela's through a third party.

121. Defendants' data collection is highly offensive and Plaintiff Montecalvo has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Montecalvo's personal browsing histories without consent.

Plaintiff Moore

122. While in California, Plaintiff Moore visited www.basspro.com on his computers and/or mobile devices.

123. During Plaintiff Moore's visits to BPS's website, Plaintiff Moore, through his computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff Moore. The communications sent by Plaintiff Moore to BPS's servers included, but were not limited to, the following actions taken by Plaintiff Moore while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted

by Plaintiff, pages and content viewed by Plaintiff Moore, scroll movement, and copy and paste actions.

124. BPS responded to Plaintiff Moore's electronic communications by supplying—through its website—the information requested by Plaintiff Moore.

125. Plaintiff Moore reasonably expected that his visit to BPS's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff Moore as he browsed, interacted with the website, and searched for products, particularly because Plaintiff Moore was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Moore that his visit to the website was being recorded by Defendants through a third party.

126. Defendants' data collection is highly offensive and Plaintiff Moore has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Moore's personal browsing histories without consent.

Plaintiff Tucker

127. While in Missouri, Plaintiff Tucker visited www.basspro.com on his mobile phone and computer.

128. During Plaintiff Tucker's visits to BPS's website, Plaintiff Tucker, through his computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff. The communications sent by Plaintiff Tucker to BPS's servers included, but were not limited to, the following actions taken by Plaintiff Tucker while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff

Tucker, pages and content viewed by Plaintiff Tucker, scroll movement, and copy and paste actions.

129. BPS responded to Plaintiff Tucker's electronic communications by supplying—through its website—the information requested by Plaintiff Tucker.

130. Plaintiff Tucker reasonably expected that his visit to BPS's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as he browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Tucker that his visit to the website was being recorded by BPS's through a third party.

131. Defendants' data collection is highly offensive and Plaintiff Tucker has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Tucker's personal browsing histories without consent.

Plaintiff Vonbergen

132. While in Pennsylvania, Plaintiff Vonbergen visited www.cabelas.com on her computer and/or smartphone approximately four times in 2022. Most recently, Plaintiff Vonbergen visited Cabela's website in or about August of 2022.

133. During her visits to Cabela's website, Plaintiff Vonbergen transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff Vonbergen. The communications sent by Plaintiff Vonbergen to Defendant's servers included, but were not limited to, the following actions taken by Plaintiff Vonbergen while on the website: mouse clicks and movements,

keystrokes, search terms, information inputted by Plaintiff, pages and content viewed by Plaintiff Vonbergen, scroll movements, and copy and paste actions.

134. Cabela's responded to Plaintiff Vonbergen's electronic communications by suppling—through its website—the information requested by Plaintiff Vonbergen.

135. Plaintiff Vonbergen reasonably expected that her visit to Cabela's website would be private and that Defendants would not have procured a third party that was tracking, recording, and/or watching Plaintiff as she browsed, interacted with the website, and searched for products, particularly because Plaintiff was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Vonbergen that her visit to the website was being recorded by Cabela's through a third party

136. Defendants' data collection is highly offensive and Plaintiff Vonbergen

has suffered concrete injury from Defendants' vast collection, aggregation and use of Plaintiff Vonbergen's personal browsing histories without consent.

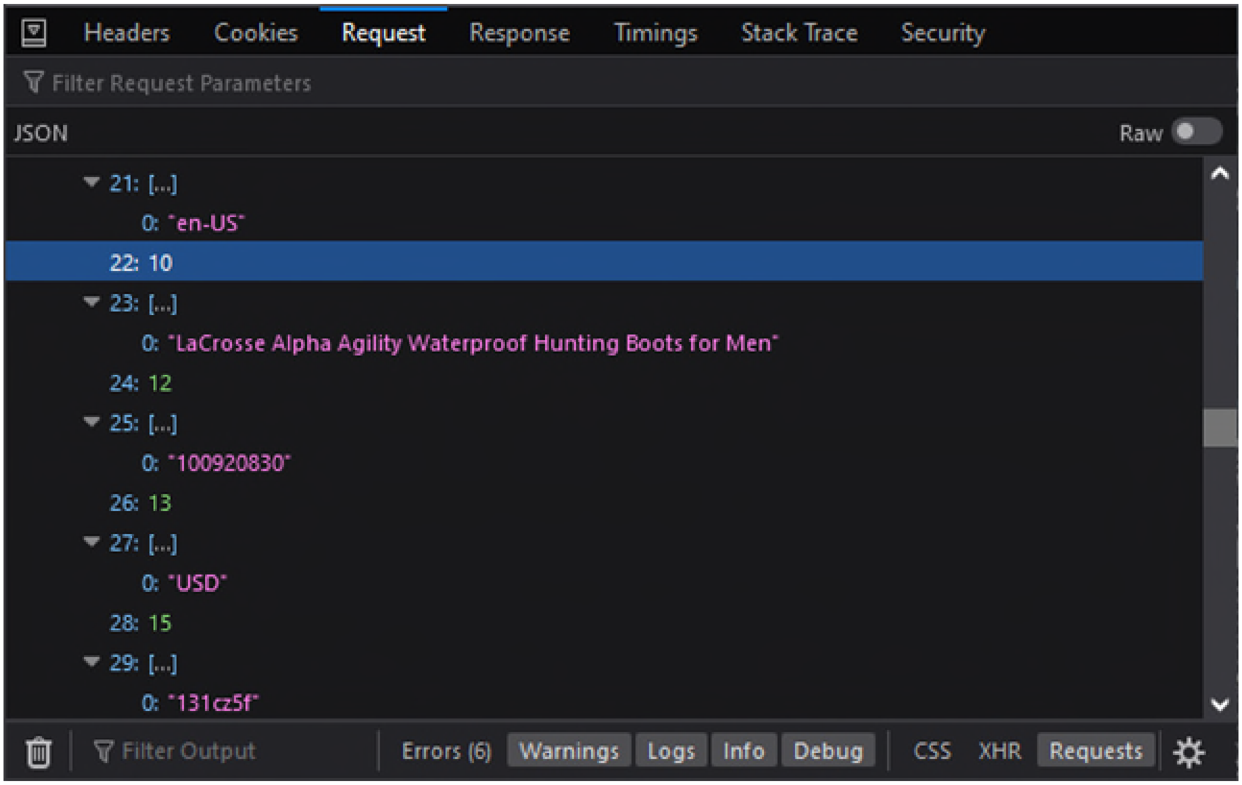
Plaintiffs' Experiences on Defendants' Websites

137. While visiting Defendants' Websites, Plaintiffs fell victim to Defendants' unlawful monitoring, recording, and collection of Plaintiffs' Website Communications with Defendants' Websites. Because, unbeknownst to Plaintiffs, Defendants procure and embed Session Replay Code on Defendants' Websites.

138. Plaintiffs' and the Class Members' Website Communications were captured automatically and instantaneously by Session Replay Code and sent to various Session Replay Providers including Microsoft, Quantum Metric, and Mouseflow.

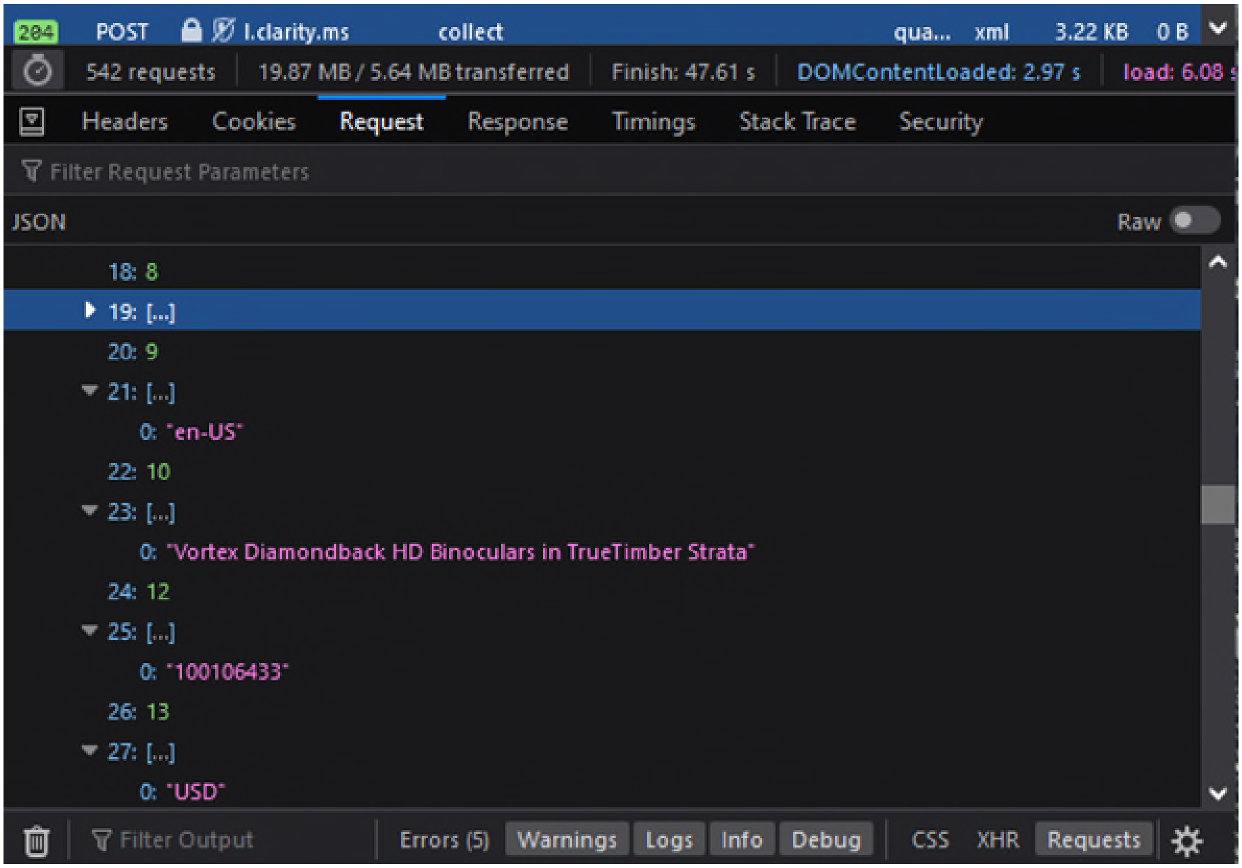
139. Further, without Plaintiffs' consent, Defendants procured Session Replay Providers, including Microsoft, Quantum Metric, and Mouseflow to obtain certain information about their devices and browser, and create a unique ID and profile for them.

140. For example, when visiting Defendants' Websites to look at a product, that information is captured by the Session Replay Code embedded on the websites:



```
▼ 21: […]
    0: "en-US"
  22: 10
▼ 23: […]
    0: "LaCrosse Alpha Agility Waterproof Hunting Boots for Men"
  24: 12
▼ 25: […]
    0: "100920830"
  26: 13
▼ 27: […]
    0: "USD"
  28: 15
▼ 29: […]
    0: "131cz5f"
```

Depicting information sent to one of the Service Replay Providers – Microsoft – through a Service Replay Code – Clarity – after viewing "LaCrosse Alpha Agility Waterproof Hunting Boots" while visiting www.cabelas.com.

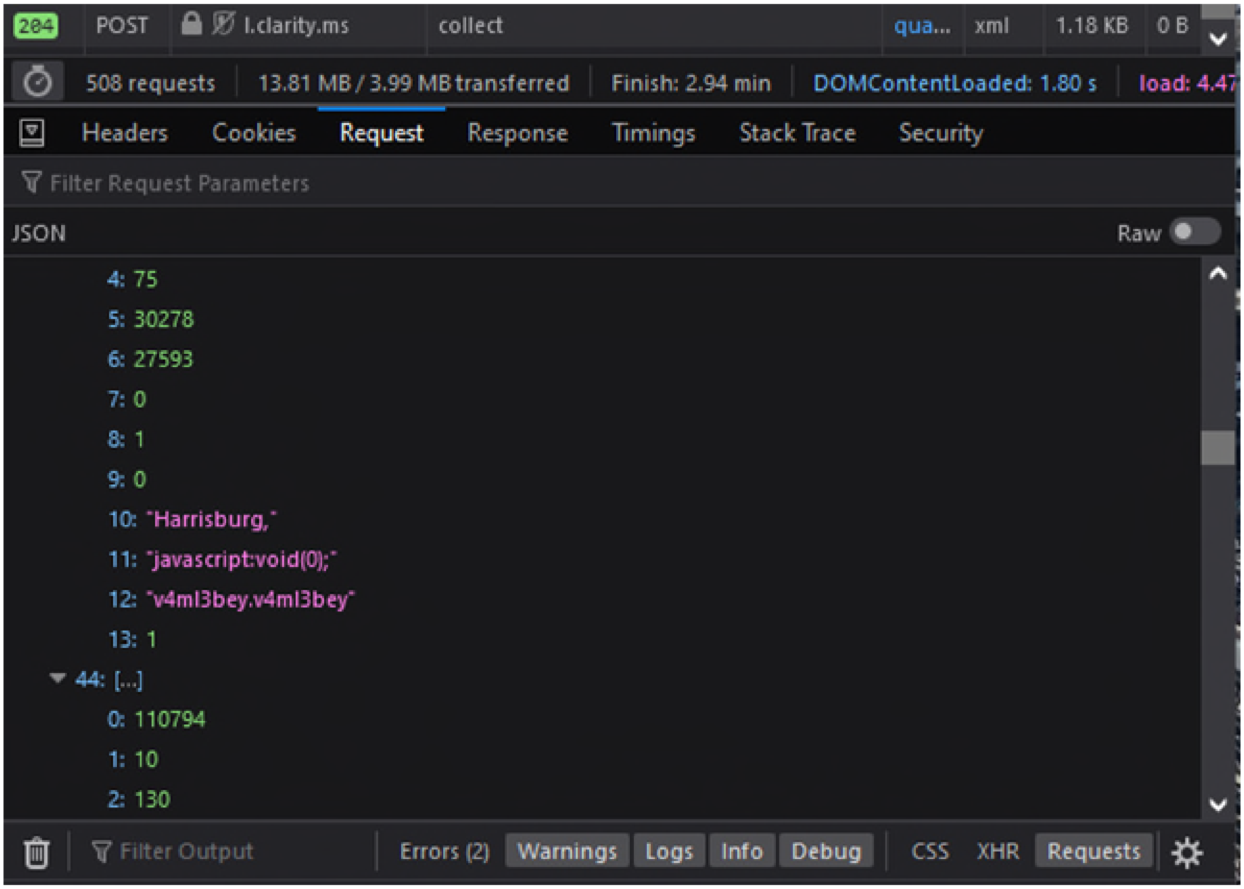


```
284  POST  l.clarity.ms  collect  qua...  xml  3.22 KB  0 B
542 requests | 19.87 MB / 5.64 MB transferred | Finish: 47.61 s | DOMContentLoaded: 2.97 s | load: 6.08
```

```
      18: 8
    ▶ 19: [...]
      20: 9
    ▼ 21: [...]
        0: "en-US"
      22: 10
    ▼ 23: [...]
        0: "Vortex Diamondback HD Binoculars in TrueTimber Strata"
      24: 12
    ▼ 25: [...]
        0: "100106433"
      26: 13
    ▼ 27: [...]
        0: "USD"
```

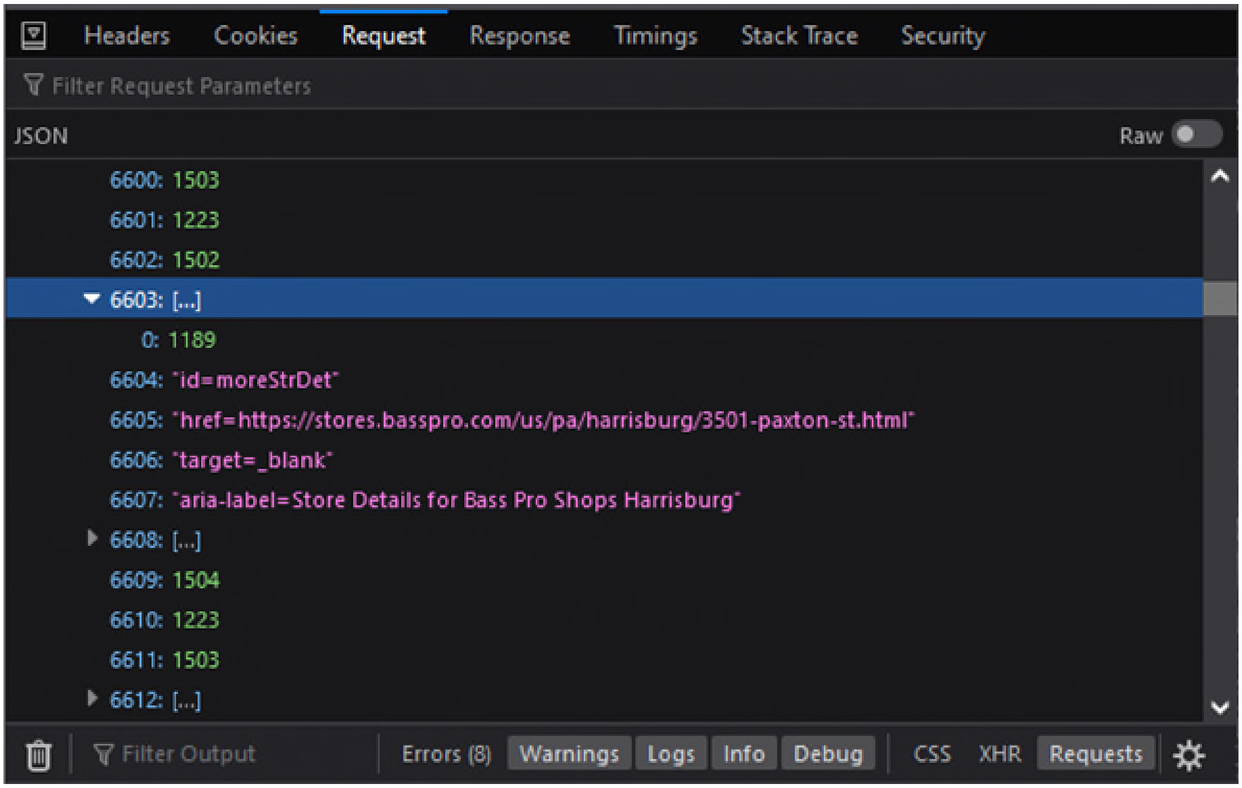
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing "Vortex Diamondback HD Binoculars in TrueTimber Strata" while visiting www.basspro.com.

141. Similarly, when website users select a store closest to them in order to view inventory and schedule in-store pick-up, that information is sent to Service Replay Providers:



```
      4: 75
      5: 30278
      6: 27593
      7: 0
      8: 1
      9: 0
      10: "Harrisburg,"
      11: "javascript:void(0);"
      12: "v4ml3bey.v4ml3bey"
      13: 1
  ▾ 44: [...]
      0: 110794
      1: 10
      2: 130
```

Depicting information sent to one of the Service Replay Providers – Microsoft – through a Service Replay Code – Clarity – after selecting "Harrisburg" as "My Store" on www.cabelas.com.

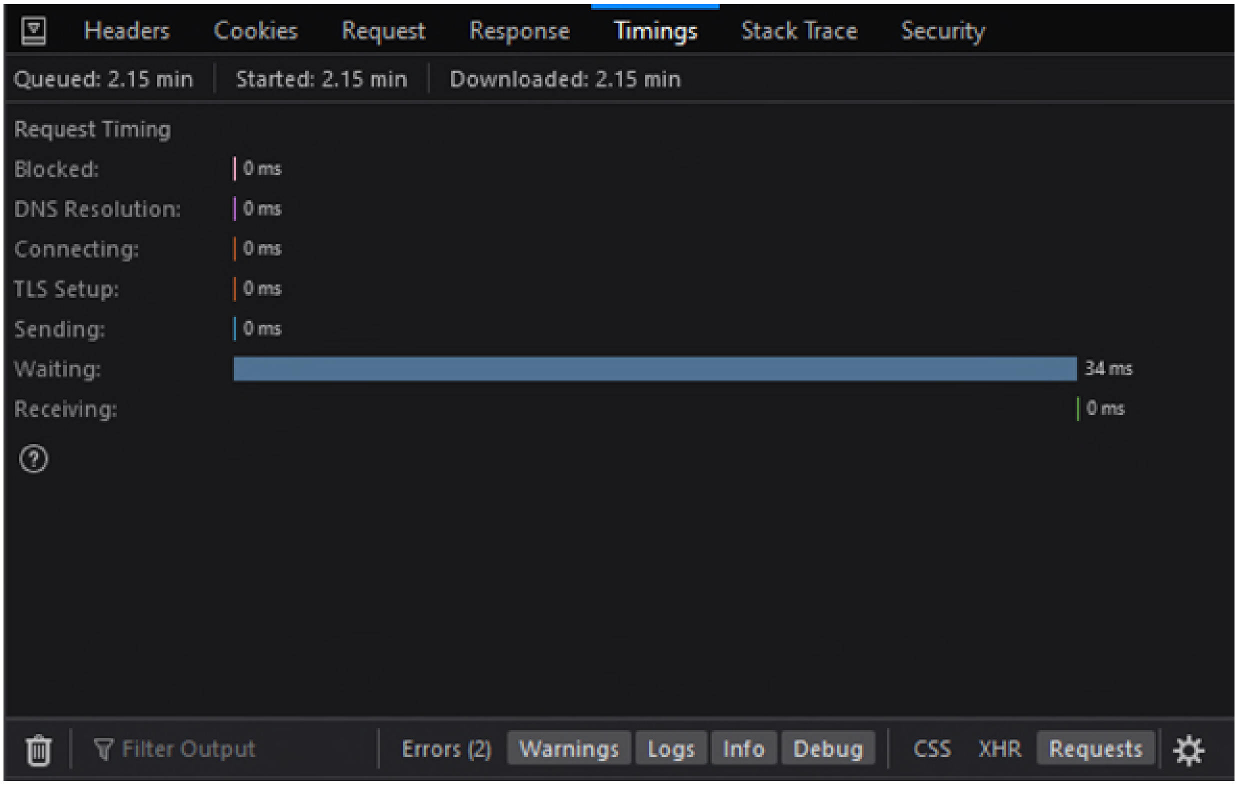


```
    6600: 1503
    6601: 1223
    6602: 1502
  ▼ 6603: [...]
      0: 1189
    6604: "id=moreStrDet"
    6605: "href=https://stores.basspro.com/us/pa/harrisburg/3501-paxton-st.html"
    6606: "target=_blank"
    6607: "aria-label=Store Details for Bass Pro Shops Harrisburg"
  ▶ 6608: [...]
    6609: 1504
    6610: 1223
    6611: 1503
  ▶ 6612: [...]
```

Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after selecting "Harrisburg" as "My Store" on www.basspro.com.

142. The wiretapping by the Session Replay Code is ongoing during the visit and intercepts the contents of these communications between Plaintiffs and Defendants with instantaneous transmissions to the Session Replay Provider, as illustrated below, in which only 34

milliseconds were required to send a packet of event response data, which would indicate whatever the website user had just done:



Queued: 2.15 min | Started: 2.15 min | Downloaded: 2.15 min

Request Timing
Blocked: 0 ms
DNS Resolution: 0 ms
Connecting: 0 ms
TLS Setup: 0 ms
Sending: 0 ms
Waiting: 34 ms
Receiving: 0 ms

143. Thus, on multiple occasions when Plaintiffs visited Defendants' Websites, the contents of their communications with Defendants' Websites were intercepted by Session Replay Code, and simultaneously transmitted to Session Replay Providers, including Microsoft, Quantum Metric, and Mouseflow.

144. The Session Replay Codes operate in the same manner for all putative Class Members.

145. Like Plaintiffs, each Class member visited one or both of Defendants' Websites with Session Replay Code embedded in them, and the Session Replay Code intercepted the Class Members' Website Communications with Defendants' Websites by sending hyper-frequent logs of those communications to Session Replay Providers.

146. Even if Defendants mask certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

147. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

148. As a specific example, if a user types a product into either Defendants' main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Defendants will repeat the searched information back on the generated page. That information will not be masked even if user-input text is fully masked in a text field.

149. The Session Replay Codes procured by Defendants are an electronic, mechanical, or other analogous device in that the Session Replay Code, monitors, collects, and records the content of electronic computer-to-computer communications between Plaintiffs' mobile computer and/or mobile device and the computer servers and hardware utilized by Defendants to operate their websites, subsequently interpreting that data to repurpose it into a Session Replay.

150. Alternatively, even if the Session Replay Code itself were not a device, the Session Replay Codes are software designed to alter the operation of a website visitor's computer or mobile phone by instructing the hardware components of that physical device to run the processes that

ultimately intercept the visitor's communications and transmit them to the third-party Session Replay Provider, without the visitor's knowledge.

151. The Session Replay Codes procured by Defendants are not website cookies, analytics tools, tags, web beacons, or other similar technologies. Instead, the data collected by the Session Replay Code identified specific information input and content viewed, and thus revealed personal and sensitive information about website visitors' internet activity and habits. As such, by the very nature of its operation, the Session Replay Code is a device used to intercept electronic communications.

152. The Website Communications intentionally monitored, collected, and recorded by Session Replay Providers procured by Defendants was content generated through Plaintiffs' and Class Members' use, interaction, and communication with Defendants' Websites relating to the substance and/or meaning of Plaintiffs' and Class Members' communications with the websites, i.e., mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiffs and Class Members, and pages and content clicked on and viewed by Plaintiffs and Class Members. This information is "content" and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed in the referrer headers. The mere fact that Defendants value this content, and procures third parties to monitor, intercept and record it, confirms these communications are content that convey substance and meaning Defendants, and in turn, any Session Replay Provider that receives the intercepted information.

F. Plaintiffs and Class Members Did Not Consent to the Interception of Their Electronic Communications

153. Plaintiffs and Class Members did not provide prior consent to Defendants' interception of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at Defendants' Websites.

154. Defendants did not ask website visitors, including Plaintiffs and Class Members, for prior consent before wiretapping their Website Communications. Indeed, Plaintiffs and Class Members have no idea upon arriving at Defendants' Websites that Defendants are using Session Replay Code to allow third parties to monitor, collect, and record their Website Communications because the Session Replay Code is seamlessly incorporated and embedded into Defendants' Websites.

155. Further, while Defendants may purport to maintain a singular "Privacy Policy" across both www.basspro.com and www.cabelas.com, the Privacy Policy is insufficient for Plaintiffs and Class Members to furnish prior consent. First, because the wiretapping begins the moment a website user visits Defendants' Websites, Plaintiffs and Class Members had no opportunity to review the Privacy Policy before they were wiretapped and therefore could not have opted out of or prevented the wiretapping before it occurred. Additionally, a reasonable person would not be on notice of the terms of Defendants' purported Privacy Policy by way of normal interaction with Defendants' Websites. Defendants' Privacy Policy is contained on the homepage of Defendants' Websites, in small low-contrasting font at the bottom of the webpages. As such, a reasonable person could browse for products on Defendants' Websites without ever being on notice of the purported Privacy Policy.

156. Similarly, Plaintiffs and Class Members did not assent to the purported "Applicable Law/Jurisdiction" clause contained in Defendants' singular Privacy Policy across both

www.basspro.com and www.cabelas.com. At no point in time during a visit to Defendants' Websites and/or their subpages is a website visitor asked to agree or even view Defendants' Privacy Policy. Moreover, Defendants' Privacy Policy is contained on the homepage of Defendants' Websites, in small low-contrasting font at the bottom of the webpages. As such, a reasonable person could browse for products on Defendants' Websites without ever being on notice of the purported Privacy Policy and/or its "Applicable Law/Jurisdiction" clause.

157. Finally, Plaintiffs and Class Members did not assent to the "Applicable Law/Jurisdiction" clause contained in Defendants' singular Terms of Use and Community Guidelines across both www.basspro.com and www.cabelas.com. At no point in time during a visit to Defendants' Websites and/or their subpages is a website visitor asked to agree or even view Defendants' Terms of Use and Community Guidelines. Moreover, Defendants' Terms of Use and Community Guidelines is contained on the homepage of Defendants' Websites, in small low-contrasting font at the bottom of the webpages. As such, a reasonable person could browse for products on Defendants' Websites without ever being on notice of the purported Terms of Use and Community Guidelines and and/or its "Applicable Law/Jurisdiction" clause.

CLASS ACTION ALLEGATIONS

158. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Nationwide Class and State Subclasses:

> **Nationwide Class:**
>
> All natural persons in the United States whose Website Communications were captured in the United States through the use of Session Replay Code embedded in Defendants' Websites.
>
> **California Subclass:**
>
> All natural persons in California whose Website Communications were captured through the use of Session Replay Code embedded in Defendants' Websites

> **Maryland Subclass:**
>
> All natural persons in Maryland whose Website Communications were through the use of Session Replay Code embedded in Defendants' Websites
>
> **Massachusetts Subclass:**
>
> All natural persons in Massachusetts whose Website Communications were captured through the use of Session Replay Code embedded in Defendants' Websites
>
> **Missouri Subclass:**
>
> All natural persons in Missouri whose Website Communications were captured through the use of Session Replay Code embedded in Defendants' Websites
>
> **Pennsylvania Subclass:**
>
> All natural persons in Pennsylvania whose Website Communications were captured through the use of Session Replay Code embedded in Defendants' Websites

159. Excluded from the Nationwide Class and Subclasses are Defendants, their parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Nationwide Class and Subclasses, the judge to whom this case is assigned, and any immediate family members thereof, and the attorneys who enter their appearance in this action.

160. **Numerosity:** The members of the Nationwide Class and Subclasses are so numerous that individual joinder of all Class Members is impracticable. The precise number of Class Members and their identities may be obtained from the books and records of Defendants or the Session Replay Providers.

161. **Commonality:** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. whether Defendants procure Session Replay Providers to intercept Defendants' Websites' visitors' Website Communications;

b. whether Defendants intentionally disclose the intercepted Website Communications of their website users;

c. whether Defendants acquire the contents of website users' Website Communications without their consent;

d. whether Defendants' conduct violates Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, California Penal Code § 631 ("CIPA"), Statutory Larceny, Cal. Pen. Code §§ 484, 496, Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, MWESA, Md. Code. Ann., Cts. & Jud. Proc. § 10-401, Massachusetts Wiretapping Statute, Mass. Gen. Laws ch. 272 §99(Q), Missouri Wiretap Act, Mo. Ann. Stat. § 542.400, *et seq.*, or WESCA, 18 Pa. C.S.A. §§ 5701, *et seq.*,

e. whether Plaintiffs and the Class Members are entitled to equitable relief; and

f. whether Plaintiffs and the Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

162. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because, among other things, all Class Members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiffs and each member of the Nationwide Class and Subclasses had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and the members of the Class typical of one another.

163. **Adequacy of Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Nationwide Class and Subclasses. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including

litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Nationwide Class and Subclasses, and Defendants have no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Nationwide Class and Subclasses, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Nationwide Class and Subclasses.

164. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class and Subclass is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

165. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiffs and each member of the Nationwide Class and Subclasses. If Defendants intercepted Plaintiffs' and Class Members' Website Communications, then Plaintiffs and each Class Member suffered damages by that conduct.

166. **Ascertainability:** Members of the Nationwide Class and Subclasses are ascertainable. Class Membership is defined using objective criteria and Class Members may be

readily identified through Defendants' books and records or the Session Replay Providers' books and records.

COUNT I
VIOLATION OF FEDERAL WIRETAP ACT
18 U.S.C. § 2510, *et. seq.*
(On behalf of the Nationwide Class)

167. Plaintiffs, individually and on behalf of a Nationwide Class, repeat and reallege each and every allegation contained above as if fully alleged herein.

168. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986, prohibits the intentional interception or attempted interception, or procurement of another for the interception, of any wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a).

169. The Wiretap Act further provides that any person who:

> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1)(c) & (d).

170. Defendants' transmission of Plaintiffs' and the Class Members' Website Communications to its Session Replay Provider(s) violates the Wiretap Act.

171. The transmission from Plaintiffs and the Class Members to Defendant, and any deployed third-party Session Replay Provider, through Defendants' Websites are communications pursuant to 18 U.S.C. § 2510(12). "Electronic communication" means *any communication* made

in whole or in part through the use of facilities for the transmission of communications by the signs, signals, writing or data between the point of origin and the point of reception. *Id.*

172. “Interception” means “the acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents… include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C.§ 2510(4), (8).

173. “Content” is broadly defined and when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication 18 U.S.C.§ 2510(8). Plaintiffs’ and the Class Members’ URLs, web page address information, mouse clicks and movements, scrolling, zooms (out or in), and text submissions (both partial and complete), including search terms or similar communications, were all collected by the Session Replay Code Defendants deployed on their websites. These constitute the contents of the electronic communications at issue.

174. “Intercepting device” or the “Electronic, mechanical or other device” means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication. U.S.C.§ 2510(5). Here, Plaintiffs’ and the Class Members’ browsers and computing devices and Defendants’ webservers, website, and the Session Replay Code Defendants deployed are all “devices” for the purposes of the Wiretap Act.

175. By deploying and embedding the Session Replay Code on Defendants’ Websites, Defendants intentionally violated the Wiretap Act, through its interception, attempt at interception, and its procurement of Session Replay Providers to intercept the content of Plaintiffs’ and the Class Members’ Website Communications.

176. Defendants also willfully used or attempted to use the contents of Plaintiffs' and the Class Members' electronic communications, knowing that the information was obtained through unlawful interception. Defendants' use of Plaintiffs' and the Class Members' information and data for advertising, revenue generating benefits, and other unknown purposes, in the absence of express written consent, or any consent, is intentionally criminal and tortious where the conduct violates state laws, including but not limited to an unlawful invasion of privacy.

177. Without Plaintiffs and Class Members' knowledge or consent, Defendants intercepted and procured Session Replay Providers, including Microsoft Clarity, Quantum Metric, and Mouseflow, to intercept the contents of their electronic communications when they navigated to the Defendants' Websites.

178. Defendants intentionally used third parties' technology—the Session Replay Code—as a means of intercepting and acquiring the contents of Plaintiffs' and Class Members' electronic communications. This violated the Wiretap Act in three primary ways. First, Session Replay Code captured and disclosed partial or unintentional text submissions to Defendants' Websites. These included communications Plaintiffs and the Class Members did not intend to send to Defendants or anyone. Second, by deploying the Session Replay Code, Defendants also procured another, the Session Replay Providers, to intercept the contents of Plaintiffs' and the Class Members Website Communications (both those intended for Defendants and not intended for Defendants) and disclosed those communications to unintended recipients to the communications (i.e., the third-party Session Replay Providers). Third, Defendants used the contents of Plaintiffs' and the Class Members' electronic communications after they were unlawfully intercepted, in violation of 18 U.S.C. § 2511(1), by Defendants and third-party Session Replay Providers for commercial gain. *See* 18 U.S.C. § 2511(1)(d).

179. No party to the communication or consent exception applies to Defendants because Defendants' conduct falls outside the scope of these exceptions and the crime-tort exception to the exception applies. *See* 18 U.S.C. § 2511(2)(d). That Section states:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d).

180. Criminal or tortious purposes include invading privacy, committing unfair business practices, committing or intent to commit trespass, or violating state computer crime laws. Defendants clearly had a criminal or tortious purpose for secretly installing and recording website users with the Session Replay Code. This Complaint asserts state law claims for invasion of privacy. Additionally, each of the states the Plaintiffs are from have computer crime laws: California, Cal. Penal Code § 502, Maryland, Md. Stat. Crim. Law § 7-302, Massachusetts, Mass. Gen. Laws ch. 266 § 33A, ch. 266 § 120F, and Pennsylvania, 18 Pa. C.S.A. §§ 7601 *et seq.*

181. Defendants' primary purpose for deploying Session Replay Code was to secretly, without permission, collect data from users. The data Session Replay Code collected from users was all encompassing, including information that users never intended to send to Defendants and certainly never intended to send an unknown, third-party Session Replay Provider. This satisfies an intent to invade users' privacy and, additionally, an intent to violate various the Computer Fraud and Abuse Act and various state computer crime laws, which generally prohibit unauthorized access to computer data, systems, and networks.

182. Defendants' interception of Plaintiffs' and the Class Members' data, and procurement of Session Replay Providers who also unlawfully intercepted Plaintiffs' and the Class

Members' data, in a manner for which they lacked permission or consent violated the Wiretap Act. Additionally, Defendants' use of the data, after it had been unlawfully intercepted, namely associating the data with users' pre-existing online activity and using it to advertise, including for direct targeted advertisements based on Plaintiffs and Class Members, violated Section 2511(1)(d), a distinct violation of the Wiretap Act, and it and of itself satisfies Section 2511(2)(d)'s unlawful purpose exception.

183. The Session Replay Providers also accessed Plaintiffs' and the Class Members' data, systems, and networks without their permission, authorization, or consent. This, too, is an unlawful interception under the Federal Wiretap Act. Defendants used the data the Session Replay Providers unlawfully intercepted for analysis and commercial gain, after it was intercepted. This constitutes a distinct violation of Section 2511(1)(d), and one which falls outside the protections purported provided in Section 2511(2)(d).

184. Pursuant to 18 U.S.C. § 2511(5)(b), for violations of the Wiretap Act, the Court "may use any means within its authority to enforce an injunction issued under paragraph (ii)(A) and shall impose a civil fine of not less than $500 for each violation of the injunction. Additionally, 18 U.S.C. § 2520 provides that "any person whose wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation of Chapter 119, may recover from the person or entity that engaged in the violation in a civil action.

185. Plaintiffs and Class Members are persons whose electronic communications were intercepted within the meaning of Section 2520. As such, they are entitled to preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual damages, punitive damages, and reasonable attorneys' fees and costs of suit.

COUNT II
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, *et seq.*
(On behalf Nationwide Class)

186. Plaintiffs, individually and on behalf of a Nationwide Class, repeat and reallege each and every allegation contained above as if fully alleged herein.

187. The Plaintiffs' and the Class's computer and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

188. Defendants exceeded, and continue to exceed, authorized access to the Plaintiffs' and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

189. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiffs' and the Class's private and personally identifiable data and content to undisclosed third parties—including the Website visitor's Electronic Communications with the website, including their finger or mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communication which were never intended for public consumption.

190. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiffs and the Class being made available to Defendant, the third-party vendor, and/or other third parties without adequate legal privacy protections.

191. Accordingly, Plaintiffs and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18

U.S.C. § 1030(g).

COUNT III
VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT
California Penal Code § 630 *et seq.*
(On behalf of the California Subclass)

192. Plaintiffs Durham and Moore ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

193. Defendants aided and abetted third party Session Replay code providers to intercept components of Plaintiffs' and California Subclass members' private electronic communications and transmissions when Plaintiffs and other Class Members accessed Defendants' Websites, and communicated thereon, from within the State of California.

194. At all relevant times to this complaint, Defendants intercepted components of Plaintiffs' and the California Subclass Members' private electronic communications and transmissions when Plaintiffs and other Subclass Members accessed Defendants' Websites within the State of California.

195. At all relevant times to this complaint, Plaintiffs and the other California Subclass Members did not know Defendants were engaging in such interception and therefore could not provide prior consent to have any part of their private electronic communications intercepted by Defendant.

196. Plaintiffs and California Subclass Members were completely unaware that Defendants had intercepted and stored electronic communications and other personal data until well after the fact and was therefore unable to consent.

197. At the inception of Defendants' illegally intercepted and unauthorized collection of Plaintiffs' and California Subclass Members' electronic communications, Defendants never

advised Plaintiffs or the other California Subclass Members that any part of these communications or their use of Defendants' Websites would be intercepted.

198. Plaintiffs and California Subclass Members were completely unaware that their use of Defendants' Websites and the electronic communications derived from such use was being intercepted and stored.

199. To establish liability under section 631(a), a plaintiff need only establish that a defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

a. Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; ***Or***

b. Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; ***Or***

c. Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; ***Or***

d. Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

200. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

201. Defendants' use of Session Replay Code amounts to spyware and is a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

202. Defendants intentionally procured Session Replay Code to automatically and secretly spy on, and intercept website visitors Website Communications in real time.

203. To facilitate this wiretap, Defendants intentionally embedded the Session Replay Code on their Websites and/or subpages.

204. By intentionally embedding Session Replay Code on their Websites and subpages, Defendants intentionally and knowingly caused Plaintiffs' and California Subclass Members' Website Communications to be intercepted, recorded, and transmitted to the Session Replay Providers.

205. By using the Session Replay Code spyware to allow others to track, record, and attempt to learn the contents of Plaintiffs' and California Subclass Members' electronic communications, Defendants knowingly and intentionally aided and abetted others to tap and learn

the contents of Plaintiffs' and California Subclass members' communications as they were in transit and being sent from or received in California.

206. These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. At the same time Plaintiffs send a GET request that is received on Defendants' servers, the same GET request is dispatched to the Session Reply Providers' servers.

207. Interception of Plaintiffs' and California Subclass Members' Website Communications occurred without their prior consent whenever they engaged with Defendants' Websites.

208. Plaintiffs and California Subclass Members had a reasonable expectation that their Website Communications would not be intercepted.

209. Plaintiffs and California Subclass members did not consent to, authorize, or know about Defendants' intrusion at the time it occurred. Plaintiffs and California Subclass members never agreed that Defendants could intercept, read, learn, collect, aid or abet others to tap and learn the content of their Website Communications.

210. Defendants intentionally intrude on Plaintiffs' and California Subclass members' private life, seclusion, or solitude, without consent, in that Defendants purposefully aided and abetted Session Replay Providers who installed code which allows Defendants and Session Replay Providers to eavesdrop and learn the content of the users' communications and other browsing activities that would otherwise be unavailable to Defendants and Session Replay Providers without engaging in this practice. Defendants directly participated in the aiding and abetting, interception,

reading, and/or learning of the contents of the communications between Plaintiffs, California Subclass Members and California-based web entities.

211. The information Session Replay Providers intercept for Defendants while Plaintiffs and California Subclass members are using their Websites includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on the Website.

212. At all relevant times, by utilizing, aiding and abetting the Session Replay Providers, Defendants willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and California Subclass Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

213. At all relevant times, Defendants agreed with, employed, and conspired with the Session Replay Providers to have the Session Replay Providers eavesdrop on Plaintiffs' and Class Members' Website communications. Indeed, by intentionally embedding Session Replay Code on their websites, Defendants aided, agreed with, and conspired with the Session Replay Providers to accomplish the wrongful conduct alleged in this complaint and violated § 631.

214. Plaintiffs and California Subclass Members did not consent to any of Defendants' actions in implementing these unauthorized connections, nor have Plaintiffs or Subclass Members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Plaintiffs' and California Subclass Members' electronic communications.

215. Plaintiffs' and the California Subclass Members' devices that Defendants accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

216. Defendants' conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

217. Plaintiffs and California Subclass Members were harmed and suffered loss by Defendants' wrongful conduct and violations, including but not limited to, violation of the right to privacy and confidentiality of their electronic communications.

218. Given the monetary value of individual personal information, Defendants deprived Plaintiffs and California Subclass Members of the economic value of their communications with Defendants' Websites, without providing proper consideration for Plaintiffs' and California Subclass Members' property.

219. Defendants have improperly profited from their invasion of Plaintiffs and California Subclass Members' privacy in the use of their data for its economic value.

220. As a result of the above violations and pursuant to CIPA section 637.2, Defendants are liable to Plaintiffs and the California Subclass Members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 provides "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

221. Defendants' conduct is ongoing, and they continue to unlawfully intercept the communications of Plaintiffs and California Subclass Members any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiffs and California

Subclass Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

222. Plaintiffs and the California Subclass Members request, as provided under CIPA, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Defendants.

COUNT IV
STATUTORY LARCENY
Cal. Pen. Code §§ 484 AND 496
(On behalf of the California Subclass)

223. Plaintiffs Durham and Moore ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

224. California Penal Code § 496(a) prohibits the obtaining of property "in any manner constituting theft." California Penal Code § 484 defines theft:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

225. Accordingly, the Cal. Pen. Code, specifically, Section 484, definition of "theft" includes obtaining property by false pretenses and provides the basis for a privacy right of action.

226. Defendants intentionally employed a program procured from third parties that would obtain personal private information under a false purpose, through deception and without the knowledge of Plaintiffs or the California Subclass Members, and in doing so, deceived

Plaintiffs and California Subclass Members into providing information to Defendants and by extension to the Session Replay Providers.

227. Defendants stole, took, and/or fraudulently appropriated Plaintiffs' and California Subclass Members' personal information without their consent.

228. Defendants concealed, aided in the concealing, sold, and/or utilized Plaintiffs' and California Subclass Members' personal information obtained for Defendants' commercial purposes and the financial benefit of Defendants.

229. Defendants knowingly and intentionally committed the acts wherein they obtained by false pretense personal information because Defendants intentionally deployed the Session Replay Code that tracked Plaintiffs' and California Subclass Members' information and operated it in a manner that was concealed and/or withheld from Plaintiffs and California Subclass Members.

230. Defendants deprived Plaintiffs and California Subclass Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

231. With fraudulent intent, Defendants concealed, aided in the concealing, and/or utilized Plaintiffs' and the California Subclass Members' information for commercial purposes and to Defendants' direct financial benefit, as the reasonable and fair market value of the unlawfully obtained data can be determined in the marketplace.

232. Plaintiffs and California Subclass Members are entitled to recover the reasonable and fair market value of the unlawfully obtain personal data taken in violation of California Penal Code §§ 484 and 496.

COUNT V
VIOLATION OF THE UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code, Sections 17200, *et seq*.,
(On behalf of the California Subclass)

233. Plaintiffs Durham and Moore ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

234. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, et seq., prohibits unfair competition – meaning any unlawful, unfair, or fraudulent business act or practice; any unfair, deceptive, untrue, or misleading advertising; and any act prohibited under Business and Professions Code 17500.

235. Each Defendant is a "person as defined by Cal. Bus. & Prof. Code § 17201.

236. Defendants' unlawful, unfair, and/or fraudulent business acts and practices, Defendants engaged in acts of unlawful and/or unfair competition prohibited by Business and Professions Code 17200 *et seq*. by virtue of the acts described herein, each of which constitutes an unlawful and/or unfair business practice. The use of such unlawful and/or unfair business practices constitutes unfair competition within the meaning of Business and Professions Code.

237. The unlawful and/or unfair business practices committed by the Defendants include, but are not limited to:

a. Committing trespass to chattels;

b. Committing conversion to chattels;

c. Committing civil trespass;

d. Violating California common law;

e. Violating federal and state statutory laws;

f. Violating the FTC Act and FTC directives;

g. Engaging in conduct in which the gravity of the harm to the Plaintiffs and the California Subclass outweighs the utility of the Defendants' conduct;

h. Engaging in acts and/or practices and/or omissions that are immoral, unethical, oppressive, or unscrupulous and causes injury to consumers which outweigh its benefits;

i. Without Plaintiffs' or California Subclass Members' knowledge or consent, Defendants injected code into their websites that was capable of transmitting the substance of Plaintiffs' and California Subclass Members' communications with Defendants to unauthorized third parties and actively aided and abetted the interception, viewing, and collection of Plaintiffs' and California Subclass Members' personal information and communications so that they could be used for advertising and other purposes for Defendants' financial benefit. The information and data Defendants intercepted includes valuable personal information, including but not limited to personally identifiable information and other privileged communications and facts.

j. Failing to disclose Defendants' practices prior to implementing Session Replay Code.

238. Plaintiffs and California Subclass Members interacted with Defendants' Websites reasonably believing that their browsing activities—and any facts and information communicated to Defendants' Websites—were secure and confidential (i.e., solely between themselves and Defendants).

239. The fact that Defendants shared the personal information of their Websites' visitors with the Session Replay Providers is material information and Plaintiffs and California Subclass

Members would not have used the Websites, or insisted on better privacy controls, had Defendants disclosed this information.

240. There is no justification for Defendants' conduct other than to increase, beyond what it would have otherwise realized, their profit from the value of their information assets through the interception and acquisition of Plaintiffs' and California Subclass members' personal information. Defendants' conduct lacks justification in that Defendants have benefited from such conduct and practices while Plaintiffs and California Subclass Members have been misled as to the nature and integrity of Defendants' services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information.

241. Defendants actively concealed their tracking practices at issue and had exclusive knowledge of it, creating a duty to disclose. Defendants could have disclosed their use of Session Replay Code and obtained their visitor's affirmative consent.

242. Defendants failed to disclose this tracking practice. Its disclosure would have been a material and important factor in Plaintiffs' and California Subclass Members' actions related to their use of the Websites.

243. Defendants' secret, undisclosed, and deceptive tracking practice caused Plaintiffs and California Subclass Members to surrender more in their transactions with Defendants than they otherwise would have. Had Plaintiffs and California Subclass Members known that Defendants could and would use their in-app browser in the manner described, they would have avoided using the Websites or demanded better privacy controls, thereby avoiding this injury.

244. Defendants' conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiffs and California Subclass members. Further, Defendants' conduct narrowly benefitted their own business interests at the expense of Plaintiffs' and California

Subclass Members' fundamental privacy interests protected by statute, the California Constitution, and the common law.

245. Plaintiffs' and California Subclass Members' loss of their personal information constitutes an economic injury.

246. Plaintiffs and California Subclass Members have suffered harm in the form of lost property value, specifically the diminution of the value of their private and personally identifiable data and content.

247. Defendants' actions caused damage to and loss of Plaintiffs' and California Subclass members' property right to control the dissemination and use of their personal information and communications.

248. Plaintiffs and the California Subclass Members have a property right in their personal information, which has value to themselves as well as Defendants, and lost money or property as a result of Defendants' violations of the UCL.

249. Each and every separate act constitutes an unlawful and/or unfair business practice. Each day that Defendants engaged in each separate unlawful act, omission, or practice is a separate and distinct violation of Business and Professions Code § 17200.

250. As a direct and proximate result of the foregoing acts and practices, Defendants have received income, profits, and other benefits, which they would not have received if Defendants had not engaged in the violations of the Unfair Competition Law described in this Complaint.

251. As a direct and proximate result of the foregoing acts and practices, Defendants have obtained a competitive unfair advantage over similar businesses that have not engaged in such practices.

252. Plaintiffs have no adequate remedy at law in that damages are insufficient to protect the public from the harm caused by the conditions described in this Complaint.

253. Plaintiffs and the California Subclass Members desire to continue using Defendants' Websites, but unless injunctive relief is granted to enjoin the unlawful business practices of Defendants, Plaintiffs, the California Subclass, and the general public have no confidence that Defendants will not continue to share their personal information and substantive communications with third parties and will suffer irreparable injury and damage.

254. Plaintiffs and the California Subclass have suffered injury in fact as a result of Defendants' unlawful, unfair, and/or fraudulent acts and/or practices.

255. Plaintiffs seek to enjoin further unlawful, unfair, and/or fraudulent acts or practices by Defendant, under Cal. Bus. & Prof. Code § 17200.

256. Plaintiffs request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing its acts and/or practices which violate the UCL and to restore to Plaintiffs and the California Subclass Members any money Defendants acquired by unfair competition, including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code § 17203 and Cal. Civ. Code § 3345; and for such other relief set forth below.

COUNT VI
VIOLATION OF MARYLAND WIRETAPPING AND ELECTRONIC SURVEILLANCE ACT
Md. Code Ann., Cts. & Jud. Proc. § 10-401, *et seq*.
(On behalf of Maryland Subclass)

257. Plaintiff Hernandez ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

258. Plaintiff and Class Members visited and interacted with Defendants' Websites from their personal computers and/or mobile devices while in Maryland.

259. Unbeknownst to Plaintiff and Class Members, Defendants procure and direct Session Replay Providers to embed Session Replay Code on Defendants' Websites to surreptitiously intercept, monitor and record nearly every interaction visitors have with their websites, in real-time.

260. Maryland's Wiretapping and Electronic Surveillance Act (the "Maryland Act") makes it unlawful for private corporations, like Defendants, to (1) willfully intercept, or procure another to intercept, any wire, oral, or electronic communication; (2) willfully disclose the contents of any wire, oral, or electronic communication, ; or (3) willfully use the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication. Md. Code Ann., Cts. & Jud. Proc. § 10-401(14) & 402(a).

261. Anyone who intercepts, discloses, or uses—or procures another to intercept, disclose, or use—a wire, oral, or electronic communication in violation of the Maryland Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

262. The electronic communications of visitors to Defendants' Websites—including mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text submissions (both partial and complete), search queries, URLs of webpages visited, and other forms of a visitors' navigation and interaction with the websites ("Website Communications")—are intentionally

intercepted by the Session Replay Code procured and utilized by Defendants in violation of the Maryland Act.

263. "Intercept" is defined by the Maryland Act as any "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10) (emphasis added).

264. "Electronic Communication" is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

265. "Contents" of an electronic communication are defined broadly to include "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

266. Plaintiff's and Class Members' intercepted Website Communications constitute the "contents" of "electronic communications" within the meaning of the Maryland Act. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Website, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits. As such, Defendants intercept the "content" generated through Plaintiff's and Class Members' intended use, interaction, and electronic communication with Defendants' Websites.

267. The Session Replay Code procured and utilized by Defendants is a "device" used for the "acquisition of the contents of [] electronic [] communication[s]" within the meaning of the Maryland Act, because it intercepts, monitors, records, and collects the contents of electronic computer-to-computer communications relayed between the personal computers and/or mobile

devices of website visitors and the computer servers and hardware utilized by Defendants to operate their websites. Moreover, the Session Replay Code procured and utilized by Defendants alters the operation of the personal computers and/or mobile devices used by website visitors by instructing the hardware components of those physical devices to run the processes that ultimately intercepts the Website Communications and transmits them contemporaneously to the Session Replay Providers. By the very nature of its operation, the Session Replay Code is therefore a "device" used to intercept electronic communications within the meaning the Maryland Act.

268. Defendants violated the Maryland Act by willfully procuring and deploying Session Replay Code on their websites to spy on visitors, automatically and secretly, and ***intercept*** the content of Plaintiff's and Class Members' electronic communications with Defendants' Websites in real-time.

269. Plaintiff's and Class Members' electronic communications are intercepted contemporaneously with their transmission.

270. The Session Replay Code procured and utilized by Defendants also ***disclose*** the content of Plaintiff's and Class Members' electronic communications to the Session Replay Providers, who could then use the intercepted electronic communications to recreate simulation videos of Plaintiff's and Class Members' entire visits to Defendants' Websites.

271. Defendants willfully ***use*** the contents of Plaintiff's and Class Members' electronic communications, knowing that the data and information was obtained through unlawful interception, for purposes of targeted advertising, marketing, and other unknown revenue generating purposes. The Session Replay Code procured and utilized by Defendants deliberately intercepts, records, and collects the content of Plaintiff's and Class Members' electronic communications with Defendants' Websites for the purpose of sending targeted marketing

information, promotions, and advertisements to customers and potential customers in Maryland, including Plaintiff and Class Members. The data and information intercepted, recorded, and collected is used by Defendants to increase their marketing efficiency, advertising, and outreach efforts, rather than to keep the websites operational.

272. Plaintiff and Class Members did not consent to Defendants' surreptitious interception and recording of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at Defendants' Websites.

273. Plaintiff and Class Members have been injured by Defendants' conduct alleged herein, which injury includes violations of their privacy and the unknowing loss of control over how their personal information and communications are received, used, or disseminated and by whom. Accordingly, the imposition of statutory damages under the Maryland Act is appropriate here.

274. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410, Plaintiff and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

275. Defendants' conduct is ongoing. Defendants continue to procure and utilize Session Replay Code to unlawfully intercept, record, collect, disclose, and use the contents of electronic communications generated by website visitors—including Plaintiff and Class Members—without their prior consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT VII
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On behalf of Maryland Subclass)

276. Plaintiff Hernandez ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

277. Maryland common law recognizes the tort of invasion of privacy.

278. Plaintiff and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

279. In violation of Plaintiff's and Class Members' reasonable expectation of privacy, Defendants intentionally procured and embedded Session Replay Code on their websites to intercept and record Plaintiff's and Class Members' every move.

280. Defendants willfully intruded on Plaintiff's and Class Members' private lives, seclusion and solitude, by, for all intents and purposes, installing a recording device on their web browsers without their consent.

281. Each time Plaintiff and Class Members visited Defendants' Websites on their personal computers and/or mobile devices, the Session Replay Code procured and utilized by Defendants secretly collected their personal data in real-time for Defendants' monetary gain and without their consent.

282. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' internet activity, including the visitor's personal interests, search queries, and habits.

283. Defendants' surreptitious interception of website visitors' Website Communications therefore allowed Defendants to monitor, record, and disclose Plaintiff's and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendants' websites in real-time.

284. Upon information and belief, the Session Replay Code embedded on Defendants' websites indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

285. Plaintiff and Class Members did not consent to, authorize, or know about Defendants' procurement of Session Replay Code or intrusion at the time it occurred. Plaintiff and Class Members never agreed that Defendants could collect, disclose, or use the contents of their Website Communications.

286. Plaintiff and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

287. Defendants willfully intrude on Plaintiff's and Class Members' private life, seclusion, or solitude, without consent.

288. Defendants' conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

289. Defendants deprived Plaintiff and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

290. Plaintiff and Class Members were harmed by Defendants' wrongful conduct as Defendants' conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

291. Defendants' conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

292. Additionally, given the monetary value of individual personal information, Defendants deprived Plaintiff and Class Members of the economic value of their interactions with Defendants' websites, without providing proper consideration for Plaintiff's and Class Members' property.

293. Further, Defendants have improperly profited from their invasion of Plaintiff and Class Members' privacy in their use of their data for its economic value and Defendants' own commercial gain.

294. Upon information and belief, Defendants derive significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

295. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

296. Defendants' conduct is ongoing. Defendants continue to unlawfully procure the interception of and intercept the Website Communications of Plaintiff and Class Members any

time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT VIII
VIOLATION OF MASSACHUSETTS WIRETAPPING STATUTE
Mass. Gen. Laws ch. 272 § 99(Q)
(On behalf of the Massachusetts Subclass)

297. Plaintiff Montecalvo ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

298. Plaintiff and Class Members visited and interacted with Defendants' Websites from their personal computers and/or mobile devices while in Massachusetts.

299. Unbeknownst to Plaintiff and Class Members, Defendants procure and direct Session Replay Providers to embed Session Replay Code on Defendants' Websites to surreptitiously intercept, monitor and record nearly every interaction visitors have with their websites—including mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text submissions (both partial and complete), search queries, URLs of webpages visited, and other forms of a visitors' navigation and interaction with the websites ("Website Communications")—in real-time.

300. The Massachusetts Wiretapping Statute (the "Massachusetts Statute") prohibits private corporations, like Defendants, from (1) willfully intercepting, or procuring another to intercept, any wire or oral communication; (2) disclosing the contents of any wire or oral communication; or (3) using the contents of any wire or oral communication, knowing that the information was obtained through interception. Mass. Gen. Laws ch. 272 § 99(B)(13) & (C).

301. The Massachusetts Statute seeks to curtail "the uncontrolled development and unrestricted use of modern electronic surveillance," which the Massachusetts Legislature termed a "grave danger[] to the privacy of all citizens of the commonwealth." Mass. Gen. Laws ch. 272 § 99(A).

302. Defendants' procurement and use of Session Replay Code violates the Massachusetts Statute, which provides a civil remedy for "[a]ny aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception[.]" Mass. Gen. Laws ch. 272 § 99(Q).

303. In relevant part, "'interception' means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." Mass. Gen. Laws ch. 272 § 99(B)(4) (emphasis added).

304. "Wire Communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." Mass. Gen. Laws ch. 272 § 99(B)(1).

305. "Contents," when "used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." Mass. Gen. Laws ch. 272 § 99(B)(5).

306. An "intercepting device" is broadly defined as "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication." Mass. Gen. Laws ch. 272 § 99(B)(3).

307. Plaintiff and Class Members' Website Communications constitute "wire communications," within the meaning of the Massachusetts Statute. *See* Mass. Gen. Laws ch. 272 § 99(B)(1); *Commonwealth v. Moody*, 466 Mass. 196, 208 (2013) (definition of "wire communication" in the Massachusetts Statute is "broad[]" and encompasses "non-oral electronic transmissions"); *see also Alves v. BJ's Wholesale Club, Inc.*, No. 22-2509-BLS1, 2023 WL 4456956 (Mass. Super. June 21, 2023) ("The mouse movements, clicks, keystrokes, and other browsing activity that [Session Replay Code] records plausibly constitute an exchange of information between the website's owner and the website user.").

308. The "contents" of Plaintiff and Class Members' Website Communications are captured and recorded by the Session Replay Code embedded on Defendants' Websites, within the meaning of the Massachusetts Statute. *See* Mass. Gen. Laws ch. 272 § 99(B)(5); *Commonwealth v. Mejia*, 64 Mass. App. Ct. 238, 243 (2005) ("'Contents' . . . is defined broadly") (quoting *District Attorney for Plymouth Dist. v. New England Tel. & Tel. Co.*, 379 Mass. 586, 591-92 (1980)). The data collected by the Session Replay Code includes specific information inputted and content viewed by visitors to Defendants' Websites and therefore reveals personalized and sensitive information about the website visitors' Internet activities, including the visitors' personal interests, browsing histories and search queries.

309. Session Replay Code, like that procured and utilized by Defendants, is an "intercepting device" used for the "recording [of] wire . . . communication[s]" within the meaning of the Massachusetts Statute because it monitors, records, and collects the contents of electronic

computer-to-computer communications relayed between the personal computers and/or mobile devices of website visitors and the computer servers and hardware utilized by Defendants to operate their websites. *See Rich v. Rich*, No. BRCV200701538, 2011 WL 3672059, at *6 (Mass. Super. July 8, 2011) (key logger program was an "intercepting device" under the Massachusetts Statute "because it is capable of . . . recording a wire . . . communication.") (quoting Mass. Gen. Laws ch. 272 § 99(B)(3)); *see also Alves v. BJ's Wholesale Club, Inc.*, No. 22-2509-BLS1, 2023 WL 4456956, at *5 (Mass. Super. June 21, 2023) (citing cases).

310. Session Replay Code intercepts and captures the content of individual visitors' Website Communications in a manner that is far more active and invasive than other analytics tools like cookies, tags, or web beacons. The Session Replay Code procured and utilized by Defendants alters the operation of the personal computers and/or mobile devices used by website visitors by instructing the hardware components of those physical devices to run the processes that ultimately intercepts the Website Communications and transmits them contemporaneously to the Session Replay Providers. By the very nature of its operation, the Session Replay Code is therefore an "intercepting device" within the meaning of the Massachusetts Statute.

311. The Session Replay Code procured and utilized by Defendants deliberately intercepts, records, and collects the content of Plaintiff's and Class Members' electronic communications with Defendants' Websites for the purpose of sending targeted marketing information, promotions, and advertisements to customers and potential customers in Maryland, including Plaintiff and Class Members. The data and information intercepted, recorded, and collected is used by Defendants to increase their marketing efficiency, advertising, and outreach efforts, rather than to keep the websites operational.

312. Defendants intentionally procure and embed Session Replay Code on their websites to spy on, automatically and secretly, and intercept the Website Communications of visitors to their websites, without their consent and in real-time.

313. Plaintiff's and Class Members' Website Communications are intercepted contemporaneously with their transmission.

314. Plaintiff and Class Members did not consent to having their Website Communications wiretapped.

315. Plaintiff and Class Members have been injured by Defendants' conduct alleged herein, which injury includes violations of their privacy and the unknowing loss of control over how their personal information and communications are received, used, or disseminated and by whom. Accordingly, the imposition of statutory damages under MWESA is appropriate here.

316. Pursuant to Mass. Gen. Laws ch. 272 § 99(Q), Plaintiffs and the Class Members seek (1) actual damages but not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1000, whichever is higher; (2) punitive damages; and (3) a reasonable attorneys' fee and other litigation disbursements reasonably incurred.

317. Defendants' conduct is ongoing. Defendants continue to utilize Session Replay Code to unlawfully intercept, disclose, and use the contents of Plaintiff's and Class Members' Website Communications any time they visit Defendants' Websites, without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT IX
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
Mass. Gen. Laws ch. 214 § 1B
(On behalf of Massachusetts Subclass)

318. Plaintiff Montecalvo ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

319. Massachusetts common law recognizes the tort of invasion of privacy. The right to privacy is also embodied by statute.

320. Pursuant to Mass. Gen. Laws ch. 214 § 1B (the "Massachusetts Privacy Act"), "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy."

321. A claim asserting an invasion of privacy under the Massachusetts Privacy Act may be based on intrusion upon solitude or seclusion, *i.e.*, an infringement upon the right to be left alone. Mass. Gen. Laws ch. 214 § 1B ("The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.").

322. Each time Plaintiff and Class Members visited Defendants' Websites on their personal computers and/or mobile devices, Defendants secretly monitored, recorded, and collected their personal data, in real-time, for Defendants' monetary gain and without Plaintiff's and Class Members' consent.

323. Plaintiff's and Class Members' URLs, web page address information, mouse clicks and movements, scrolling, zooms (out or in), and text submissions (both partial and complete), including search terms or similar communications ("Website Communications"), were all collected by the Session Replay Code that Defendants procured and deployed on their websites.

324. Plaintiff and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

325. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits.

326. Defendants' surreptitious interception of website visitors' Website Communications therefore allowed Defendants to monitor, record, and disclose Plaintiff's and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendants' Websites in real-time.

327. Upon information and belief, the Session Replay Code embedded on Defendants' Websites indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

328. Plaintiff and Class Members did not consent to, authorize, or know about Defendants' intrusion at the time it occurred. Plaintiff and Class Members never agreed that Defendants could collect, disclose, or use the contents of their Website Communications.

329. Plaintiff and Class Members had an objective interest in conducting their personal activities without intrusion or interference and precluding the installation and embedding of the Session Replay Code on their devices for the purpose of disseminating and/or misusing their information and communications. This includes the right to not have their personal devices violated and personal information intercepted and utilized for business gain.

330. Defendants intentionally intrude on Plaintiff's and Class Members' private life, seclusion, or solitude, without consent.

331. Defendants' conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

332. Defendants deprived Plaintiff and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

333. Plaintiff and Class Members were harmed by Defendants' wrongful conduct as Defendants' conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their personal information.

334. Defendants' conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure, and loss of privacy and confidentiality, has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

335. Additionally, given the monetary value of individual personal information, Defendants deprived Plaintiff and Class Members of the economic value of their interactions with Defendants' Websites, without providing proper consideration for Plaintiff's and Class Members' property.

336. Further, Defendants have improperly profited from their invasion of Plaintiff's and Class Members' privacy by using Plaintiff's and Class Members' personal data and information for its economic value and Defendants' own commercial gain.

337. Upon information and belief, Defendants derive significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

338. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

339. Defendants' conduct is ongoing. Defendants continue to unlawfully intercept the Website Communications of Plaintiffs and Class Members any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT X
VIOLATION OF MISSOURI WIRETAP ACT,
Mo. Ann. Stat. §§ 542.400 *et seq.*
(On behalf of the Missouri Subclass)

340. Plaintiff Tucker ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

341. Plaintiff and Class Members visited and interacted with Defendants' Websites from their personal computers and/or mobile devices while in Missouri.

342. Unbeknownst to Plaintiff and Class Members, Defendants procure and direct Session Replay Providers to embed Session Replay Code on Defendants' Websites to surreptitiously intercept, monitor and record nearly every interaction visitors have with their websites—including mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text submissions (both partial and complete), search queries, URLs of webpages visited, and other forms of a visitors' navigation and interaction with the websites ("Website Communications")—in real-time.

343. The Missouri Wiretap Act broadly prohibits the interception, disclosure, or use of any wire, oral or electronic communication. Mo. Stat. § 542.402. Defendants' procurement and use of the Session Replay Code violates the Missouri Wiretap Act, which provides a civil remedy for "[a]ny person whose wire communication is intercepted, disclosed, or used in violation of

sections 542.00 to 542.422[, who] shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications; and (2) be entitled to recover from any such person: (a) actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation or ten thousand dollars whichever is greater; (b) punitive damages on a showing of a willful or intentional violation of sections 542.400 to 542.422; and (c) a reasonable attorney's fee and other litigation costs reasonably incurred. Mo. Stat. § 542.218.

344. "Intercept" is defined as "the aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device[.]" Mo. Stat. § 542.200(6).

345. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications." Mo. Stat. § 542.200(12).

346. "Contents," "when used with respect to any wire communication, includes any information concerning the identity of the parties, the substance, purport, or meaning of that communication." Mo. Stat. § 542.200(3).

347. "Electronic, mechanical, or other device" is broadly defined to include "any device or apparatus which can be used to intercept a wire communication[.]" Mo. Stat. § 542.200(5).

348. Plaintiff and Class Members' Website Communications constitute "wire communications," within the meaning of the Missouri Wiretap Act. *See* Mo. Stat. § 542.200(12). The mouse movements, clicks, keystrokes, and other browsing activity recorded by the Session

Replay Code embedded on Defendants' websites constitute an exchange of information between the website's owner and the website user that is encompassed by the broad definition of "wire communications" in the Missouri Wiretap Act ("any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, *or other like connection* between the point of origin and the point of reception") (emphasis added).

349. Plaintiff's and Class Members' intercepted Website Communications constitute the "contents" of "wire communications" within the meaning of the Missouri Wiretap Act. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits. As such, Defendants intercept the "content" generated through Plaintiff's and Class Members' intended use, interaction, and communication with Defendants' Websites.

350. The Session Replay Code procured and utilized by Defendants is an "electronic, mechanical or other device" used to transcribe electronic communications and to intercept wire communications within the meaning of the Missouri Wiretap Act, because it intercepts, monitors, records, and collects the contents of computer-to-computer communications relayed between the personal computers and/or mobile devices of website visitors and the computer servers and hardware utilized by Defendants to operate their websites. Moreover, the Session Replay Code procured and utilized by Defendants alters the operation of the personal computers and/or mobile devices used by website visitors by instructing the hardware components of those physical devices to run the processes that ultimately intercepts the Website Communications and transmits them contemporaneously to the Session Replay Providers. By the very nature of its operation, the

Session Replay Code is therefore a “device” used to intercept electronic communications within the meaning the Missouri Wiretap Act.

351. Plaintiff and Class Members were not aware that Defendants and the other Session Replay Providers were intercepting and recording their Website Communications.

352. Defendants violated the Missouri Wiretap Act by intentionally procuring and deploying Session Replay Code on their websites to spy on visitors, automatically and secretly, and ***intercept*** the content of Plaintiff’s and Class Members’ private electronic communications with Defendants’ Websites, in real time.

353. Plaintiff’s and Class Members’ private electronic communications were intercepted contemporaneously with their transmission.

354. The Session Replay Code procured and utilized by Defendants also ***discloses*** the content of Plaintiff’s and Class Members’ communications to the Session Replay Providers, who could then use the intercepted electronic communications to recreate simulation videos of Plaintiff’s and Class Members’ entire visits to Defendants’ Websites.

355. Defendants willfully ***use*** the contents of Plaintiff’s and Class Members’ electronic communications, knowing that the data and information was obtained through unlawful interception, for purposes of targeted advertising, marketing, and other unknown revenue generating purposes. The Session Replay Code procured and utilized by Defendants deliberately intercepts, records, and collects the content of Plaintiff’s and Class Members’ electronic communications with Defendants’ Websites for the purpose of sending targeted marketing information, promotions, and advertisements to customers and potential customers in Missouri, including Plaintiff and Class Members. The data and information intercepted, recorded, and

collected is used by Defendants to increase their marketing efficiency, advertising, and outreach efforts, rather than to keep the websites operational.

356. Plaintiff and Class Members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class Members.

357. Plaintiff and Class Members did not consent to Defendants' surreptitious interception and recording of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at Defendants' Websites.

358. Under the Missouri Wiretap Act, "[i]t is not unlawful . . . [f]or a person not acting under law to intercept a wire communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception **unless such communication is intercepted for the purpose of committing any criminal or tortious act**." Mo. Stat. § 542.402.1(1), 2(3) (emphasis added).

359. Defendants procured, intercepted, recorded, and collected Plaintiff's and Class Members' Website Communications for the purpose of committing a tortious act, namely, to invade the privacy of Plaintiff and Class Members.

360. Moreover, the third-party Session Replay Providers are not parties to Plaintiff and Class Members' Website Communications. The Session Replay Code procured and utilized by Defendants captures, records and transmits a broad range of data and information to the Session Replay Providers, including information that Plaintiff and Class Members never intended to send to Defendants, much less to unknown, third-party Session Replay Providers.

361. Plaintiff and Class Members have been injured by Defendants' conduct alleged herein, which injury includes violations of their privacy and the unknowing loss of control over

how their personal information and communications are received, used, or disseminated and by whom. Accordingly, the imposition of statutory damages under the Missouri Wiretap Act is appropriate here.

362. Pursuant to Mo. Stat. § 542.418, Plaintiff and Class Members are entitled to: (1) actual damages; (2) statutory damages including liquidated damages at $100 per day of violation or $10,000, whichever is greater, and (3) punitive damages. Plaintiff- and Class Members are also entitled to an award of attorney's fees and expenses.

363. Defendants' conduct is ongoing. Defendants continue to procure and utilize Session Replay Code to unlawfully intercept, record, collect, disclose, and use the contents of communications generated by website visitors—including Plaintiff and Class Members—any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT XI
VIOLATION OF MISSOURI'S MERCHANDISING PRACTICES ACT,
Mo. Rev. Stat. § 407.010 *et seq.*
(On behalf of the Missouri Subclass)

364. Plaintiff Tucker ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

365. The Missouri Merchandising Practice Act (the "MPA") prohibits false, fraudulent or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

366. The MPA prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment,

suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

367. Plaintiff, individually and on behalf of the Class, is entitled to bring this action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.020, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

368. Defendants are "person[s]" within the meaning of the MPA in that Defendants are domestic "[…] for-profit […] corporation[s]." Mo. Rev. Stat. § 407.010(5).

369. The Session Replay Providers are "person[s]" within the meaning of the MPA because they are domestic "[…] for-profit […] corporation[s]." Mo. Rev. Stat. § 407.010(5).

370. Plaintiff and Class Members are "persons" under the MPA because they are natural persons and they visited Defendants' websites for personal, family, and/or household use.

371. The Missouri Attorney General has promulgated regulations defining the meaning of unfair practice as used in the MPA. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

a. An unfair practice is any practice which—

i. Either—

1. Offends any public policy as it has been established by the Constitution, statutes, or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive, or unscrupulous; and

ii. Presents a risk of, or causes, substantial injury to consumers.

b. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See, Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365).

372. Pursuant to the MPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendants' acts and omissions fall within the meaning of "unfair."

373. Missouri case law provides that the MPA's "literal words cover *every practice imaginable and every unfairness to whatever degree*." *Conway v. CitiMortgage, Inc.*, 438S.W.3d 410, 416 (Mo. 2014) (quoting *Ports Petroleum Co., Inc. of Ohio v. Nixon*, 37 S.W.3d237, 240 Mo. banc 2001). Furthermore, the statute's "plain and ordinary meaning of the words themselves are unrestricted, all-encompassing and exceedingly broad." *Id.* at 240.

374. Defendants violated the MPA by omitting and/or concealing material facts about Defendants' websites and/or engaging in unfair or deceptive trade practices in their operation of their websites. Notably, Defendants omitted and/or concealed that they directed Session Replay Providers to secretly monitor, collect, transmit, and disclose their website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

375. Defendants' procurement, direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on Defendants' Websites. Defendants do not disclose their use of Session Replay Code to secretly monitor and collect website visitors'

Website Communications. Had Plaintiff and Class Members known that the Session Replay Code (that collects, transmits, and discloses Website Communications to the Session Replay Providers) was embedded in Defendants' Websites, they would not have visited Defendants' Websites to shop for, purchase, or contract to purchase goods and merchandise, or they would have required Defendants to compensate them for the interception, collection, and disclosure of their Website Communications.

376. Defendants' intentional concealment of the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in Defendants' websites is material because Defendants know that consumers would not otherwise visit their websites to search for, purchase, and contract to purchase goods and merchandise. Indeed, Defendants' concealment of such facts was intended to mislead consumers.

377. Defendants' concealment, suppression, and/or omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MPA.

378. By failing to disclose and inform Plaintiff and Class Members about their interception, collection, and disclosure of website visitors' Website Communications, Defendants engaged in acts and practices that constitute unlawful practices in violation of the MPA. Mo. Ann. Stat. §§ 407.010, *et seq*.

379. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Defendants. The collection and use of Plaintiff and Class Members' personal data and information has now diminished the value of such data and information to Plaintiff and the Class.

380. As such, Plaintiff and the Class seek an order (1) requiring Defendants to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs. Plaintiff and the Class seek all relief available under Mo. Ann. Stat. § 407.020, which prohibits "the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce[,]" as further interpreted by Mo. Code Regs. Ann. tit. 15, §§ 60-7.010, *et seq*., Mo. Code Regs. Ann. tit. 15, §§ 60-8.010, *et seq*., and Mo. Code Regs. Ann. tit. 15, §§ 60-9.010, *et seq.,* and Mo. Ann. Stat. § 407.025, which provides for the relief sought in this count.

381. Defendants' conduct is ongoing. Defendants continue to procure and utilize Session Replay Code to unlawfully intercept, record, collect, disclose, and use the contents of electronic communications generated by website visitors—including Plaintiff and Class Members—any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT XII
INVASION OF PRIVACY – MISSOURI INTRUSION UPON SECLUSION
(On behalf of the Missouri Subclass)

382. Plaintiff Tucker ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

383. Missouri common law recognizes the tort of invasion of privacy, including claims for unreasonable intrusion upon the seclusion of another.

384. Plaintiff and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

385. In violation of Plaintiff's and Class Members' reasonable expectation of privacy, Defendants intentionally procured, used, and embedded Session Replay Code on their websites to intercept and record Plaintiff's and Class Members' every move.

386. Defendants willfully intruded on Plaintiff's and Class Members' private lives, seclusion and solitude, by, for all intents and purposes, installing a recording device on their web browsers without their consent.

387. Each time Plaintiff and Class Members visited Defendants' Websites on their personal computers and/or mobile devices, the Session Replay Code procured and utilized by Defendants secretly collected their personal data in real-time for Defendants' monetary gain and without their consent.

388. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits.

389. Defendants' procurement of and surreptitious interception of website visitors' Website Communications therefore allowed Defendants to monitor, record, and disclose Plaintiff's and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendants' Websites in real-time.

390. Upon information and belief, the Session Replay Code embedded on Defendants' Websites indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

391. Plaintiff and Class Members did not consent to, authorize, or know about Defendants' intrusion at the time it occurred. Plaintiff and Class Members never agreed that Defendants could collect, disclose, or use the contents of their Website Communications.

392. Plaintiff and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

393. Defendants intentionally intruded on Plaintiff's and members' private life, seclusion, or solitude, without consent.

394. Defendants' conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

395. Defendants deprived Plaintiff and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

396. Plaintiff and Class Members were harmed by Defendants' wrongful conduct, and Defendants' conduct has caused Plaintiff and Class Members mental anguish and suffering arising, from their loss of privacy and confidentiality of their electronic communications.

397. Defendants' conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff and the Class Members to experience mental anguish, emotional distress, worry, fear, and other harms.

398. Additionally, given the monetary value of individual personal information, Defendants deprived Plaintiff and Class Members of the economic value of their interactions with

Defendants' Websites, without providing proper consideration for Plaintiff's and Class Members' property.

399. Further, Defendants have improperly profited from their invasion of Plaintiff's and Class Members' privacy in their use of Plaintiff and Class Members' personal information and data for its economic value and Defendants' own commercial gain.

400. Upon information and belief, Defendants derive significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

401. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

402. Defendants' conduct is ongoing. Defendants continue to unlawfully intercept the Website Communications of Plaintiff and Class Members any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT XIII
VIOLATION OF PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT,
18 Pa. C.S.A. §§ 5701, *et seq.*
(On behalf of the Pennsylvania Subclass)

403. Plaintiffs Calvert, Cornell, and Vonbergen ("Plaintiffs," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

404. Plaintiffs and Class Members visited and interacted with Defendants' Websites from their personal computers and/or mobile devices while in Pennsylvania.

405. Unbeknownst to Plaintiffs and Class Members, Defendants procure and direct Session Replay Providers to embed Session Replay Code on Defendants' Websites to surreptitiously intercept, monitor and record nearly every interaction visitors have with their websites, in real-time.

406. WESCA makes it unlawful for private corporations, like Defendants, to (1) intentionally intercept, or procure another to intercept, any wire, electronic, or oral communication; (2) intentionally disclose the contents of any wire, electronic, or oral communication; or (3) intentionally use the contents of any wire, electronic, or oral communication, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. C.S.A. § 5703.

407. Defendants' procurement and use of the Session Replay Code violates WESCA, which provides a civil remedy for "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used[.]". 18 Pa. C.S.A. § 5725(a).

408. The Website Communications of visitors to Defendants' websites—including mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text submissions (both partial and complete), search queries, URLs of webpages visited, and other forms of a visitors' navigation and interaction with the websites—are intentionally intercepted by the Session Replay Code procured and utilized by Defendants in violation WESCA.

409. "Intercept" is defined as any "[a]ural or other acquisition of the contents of *any wire, electronic or oral communication* through the use of *any electronic, mechanical or other device*." 18 Pa. C.S.A. § 5702 (emphasis added).

410. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. C.S.A. § 5702.

411. "Contents," when "used with respect to [] electronic [] communication[s], is any information concerning the substance, purport, or meaning of that communication." 18 Pa. C.S.A. § 5702.

412. Plaintiffs' and Class Members' intercepted Website Communications constitute the "contents" of "electronic communications" within the meaning of WESCA. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits. As such, Defendants intercept the "content" generated through Plaintiffs' and Class Members' intended use, interaction, and electronic communication with Defendants' Websites.

413. The Session Replay Code procured and utilized by Defendants is a "device" used for the "acquisition of the contents of [] electronic [] communication[s]" within the meaning of WESCA, because it intercepts, monitors, records, and collects the contents of electronic computer-to-computer communications relayed between the personal computers and/or mobile devices of website visitors and the computer servers and hardware utilized by Defendants to operate their websites. Moreover, the Session Replay Code procured and utilized by Defendants alters the operation of the personal computers and/or mobile devices used by website visitors by instructing the hardware components of those physical devices to run the processes that ultimately intercepts the Website Communications and transmits them contemporaneously to the Session Replay Providers. By the very nature of its operation, the Session Replay Code is therefore a "device"

used to intercept electronic communications within the meaning of WESCA. Alternatively, Plaintiffs' hardware is the "device" controlled by the Session Replay Code used to intercept electronic communications within the meaning of WESCA.

414. Defendants violated WESCA by intentionally procuring and deploying Session Replay Code on their websites to spy on visitors, automatically and secretly, and ***intercept*** the content of Plaintiffs' and Class Members' electronic communications with Defendants' Websites in real-time.

415. Plaintiffs' and Class Members' electronic communications are intercepted contemporaneously with their transmission.

416. The Session Replay Code procured and utilized by Defendants also ***discloses*** the content of Plaintiffs' and Class Members' electronic communications to the Session Replay Providers, who could then use the intercepted electronic communications to recreate simulation videos of Plaintiffs' and Class Members' entire visits to Defendants' Websites.

417. Defendants intentionally ***use*** the contents of Plaintiffs' and Class Members' electronic communications, knowing that the data and information was obtained through unlawful interception, for purposes of targeted advertising, marketing, and other unknown revenue generating purposes. The Session Replay Code procured and utilized by Defendants deliberately intercepts, records, and collects the content of Plaintiffs' and Class Members' electronic communications with Defendants' Websites for the purpose of sending targeted marketing information, promotions, and advertisements to customers and potential customers in Pennsylvania, including Plaintiffs and Class Members. The data and information intercepted, recorded, and collected is used by Defendants to increase their marketing efficiency, advertising, and outreach efforts, rather than to keep the websites operational.

418. Plaintiffs and Class Members did not consent to Defendants' surreptitious interception and recording of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at Defendants' websites.

419. Plaintiffs and Class Members have been injured by Defendants' conduct alleged herein, which injury includes violations of their privacy and the unknowing loss of control over how their personal information and communications are received, used, or disseminated and by whom. Accordingly, the imposition of statutory damages under WESCA is appropriate here.

420. Pursuant to 18 Pa. C.S.A. 5725(a), Plaintiffs and Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

421. Defendants' conduct is ongoing. Defendants continue to procure and utilize Session Replay Code to unlawfully intercept, record, collect, disclose, and use the contents of electronic communications generated by website visitors—including Plaintiffs and Class Members—any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiffs and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT XIV
INVASION OF PRIVACY – PENNSYLVANIA INTRUSION UPON SECLUSION
(On behalf of the Pennsylvania Subclass)

422. Plaintiffs Calvert, Cornell, and Vonbergen ("Plaintiffs," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

423. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

424. Each time Plaintiffs and Class Members visited Defendants' Websites on their personal computers and/or mobile devices, Defendants secretly monitored, recorded, and collected their personal data, in real-time, for Defendants' monetary gain and without Plaintiffs' and Class Members' consent.

425. Plaintiffs and Class Members' URLs, web page address information, mouse clicks and movements, scrolling, zooms (out or in), and text submissions (both partial and complete), including search terms or similar communications ("Website Communications"), were all collected by the Session Replay Code that Defendants procured and deployed on their websites.

426. Plaintiffs and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

427. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendants' Websites, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits.

428. Defendants' surreptitious procurement and interception of website visitors' Website Communications therefore allowed Defendants to monitor, record, and disclose Plaintiffs' and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendants' Websites in real-time.

429. Upon information and belief, the Session Replay Code embedded on Defendants' Websites indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

430. Plaintiffs and Subclass Members did not consent to, authorize, or know about Defendants' intrusion at the time it occurred. Plaintiffs and Class Members never agreed that Defendants could collect, disclose, or use the contents of their Website Communications.

431. Plaintiffs and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

432. Defendants intentionally intrude on Plaintiffs' and Class Members' private life, seclusion, or solitude, without consent.

433. Defendants' conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

434. Defendants deprived Plaintiffs and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

435. Plaintiffs and Class Members were harmed by Defendants' wrongful conduct as Defendants' conduct has caused Plaintiffs and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their personal information.

436. Defendants' conduct has needlessly harmed Plaintiffs and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiffs and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

437. Additionally, given the monetary value of individual personal information, Defendants deprived Plaintiffs and Class Members of the economic value of their interactions with

Defendants' Websites, without providing proper consideration for Plaintiffs' and Class Members' property.

438. Further, Defendants have improperly profited from their invasion of Plaintiffs' and Class Members' privacy by using Plaintiffs' and Class Members personal data and information for its economic value and Defendants' own commercial gain.

439. Upon information and belief, Defendants derive significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

440. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

441. Defendants' conduct is ongoing. Defendants continue to unlawfully procure the interception and to unlawfully intercept the Website Communications of Plaintiffs and Class Members any time they visit Defendants' Websites with Session Replay Code enabled without their consent. Plaintiffs and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT XV
TRESPASS TO CHATTELS
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative the Missouri, California, Maryland, Pennsylvania and Massachusetts Classes)

442. Plaintiffs repeat and reallege each and every allegation contained above as if fully alleged herein. For purposes of this Count, "Plaintiffs and the Classes" means Plaintiffs and the Nationwide Class, or, in the alternative, the Missouri, California, Maryland, Pennsylvania and Massachusetts Subclasses.

443. Plaintiffs and the Classes owned, possessed, and/or had a right to possess Plaintiffs' devices (i.e., their mobile device or computer) and/or the data contained therein.

444. Plaintiffs' and Class Members' devices are chattel in that the devices are tangible, movable, and transferable.

445. Plaintiffs' and Class Members' data is also valuable chattel that is tangible or intangible and is movable and transferrable.

446. As set forth above, Defendants intentionally, directly or through a third party, interfered with; intermeddled with; used; took; transferred from Plaintiffs and the Classes; and/or exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data contained on Plaintiffs' devices as described above.

447. As to the devices, Defendants used Plaintiffs' and Class Members' devices by causing a third party to place Session Replay Code directly on Plaintiffs' and the Classes devices for the purpose of tracking all of the user's interactions with the website that it wouldn't have been able to track had it not placed the Session Replay Code on the device and engaged in this surreptitious tracking. Defendants caused a third party to transfer Plaintiffs' data from Plaintiffs' devices to the Cloud Storage Data Centers of the Session Replay Providers. Defendants exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the devices by placing the Session Replay Code to stalk users of their websites.

448. As to the data, Defendants used Plaintiffs' and Class Members' data by transferring it from Plaintiffs' device to the Cloud Storage Data Centers of the Session Replay Providers for the purpose of using the data to make money without paying for it. Defendants exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data by capturing, taking, and/or using the data without permission or consent from Plaintiffs and the

Classes.

449. Plaintiffs' data that was transferred from Plaintiffs' and Class Members' respective devices are maintained in cloud storage devices located on servers across the nation.

450. For example, Clarity data is stored in the Microsoft Azure cloud service.[43] The Azure Cloud Data Center locations (which host their services) are located across the United States and elsewhere.[44]

451. Microsoft provides the following only regarding the Azure cloud service it offers to Session Replay Providers:

> As a customer, you *maintain ownership of customer data*—the content, personal and other data you provide for storing and hosting in Azure services. You are also in control of any additional geographies where you decide to deploy your solutions or replicate your data."[45]

452. Quantum Metric stores data on the Google Cloud Platform.[46] Google Cloud is located in 9 locations in the US alone.[47] Google represents:

> Rather than storing each user's data on a single machine or set of machines, we distribute all data — including our own — across many computers in different locations.[48]

453. As such, Plaintiffs' and Class Members' data is tied to something tangible – i.e., Microsoft Azure and/or Google Servers.

[43] https://learn.microsoft.com/en-us/clarity/faq

[44] https://datacenterlocations.com/microsoft-azure/#USA

[45] https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency/#overview (emphasis added).

[46] https://www.quantummetric.com/platform-foundations/data-privacy-security/

[47] https://cloud.google.com/about/locations#americas

[48] *See* https://www.google.com/about/datacenters/data-security/

454. All Session Replay Providers operate in a similar manner with cloud devices and servers.

455. Plaintiffs and the Classes did not consent to the aforementioned intermeddling and/or interference.

456. The aforementioned intermeddling and/or interference was the actual and proximate cause of injury to Plaintiffs and the Classes because it exposed their respective private data and/or personally identifiable information and/or other data to one or more third parties.

457. Additionally, the interference gave third parties the data and information without the consent of Plaintiffs and the Classes and which is valuable and for which Defendants did not obtain informed consent nor pay Plaintiffs or the Classes to obtain.

458. Plaintiffs and the Classes members are entitled to recover the actual damages they suffered as a result of Defendants' aforementioned interference with their respective computer and/or mobile devices in an amount to be determined at trial.

COUNT XVI
CONVERSION TO CHATTELS
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative the California, Missouri, Maryland, Pennsylvania and Massachusetts Classes)

459. Plaintiffs repeat and reallege each and every allegation contained above as if fully alleged herein. For purposes of this Count, "Plaintiffs and the Classes" or "Plaintiffs and Class Members" means Plaintiffs and the Nationwide Class, or, in the alternative, the Missouri, California, Maryland, Pennsylvania and Massachusetts Classes.

460. Plaintiffs and the Classes owned, possessed, and/or had a right to possess Plaintiffs' devices (i.e., their mobile device or computer) and/or the data contained therein.

461. Plaintiffs' and Class Members' devices are chattel in that the devices are tangible, movable, and transferrable.

462. Plaintiffs' and Class Members' data is also valuable chattel that is tangible or intangible and is movable and transferrable.

463. As set forth above, Defendants intentionally, directly or through a third party, interfered with; intermeddled with; used; took; transferred from Plaintiffs and the Classes; and/or exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data contained on Plaintiffs' devices as described above.

464. As to the devices, Defendants used Plaintiffs' and Class Members' devices by placing Session Replay Code directly on Plaintiffs' and the Classes devices for the purpose of tracking all of the user's interactions with the website that it wouldn't have been able to track had it not placed the Session Replay Code on the device and engaged in this surreptitious tracking. Session Replay Code embedded by Defendants transferred from Plaintiffs' device Plaintiffs' data to the Cloud Storage Data Centers of the Session Replay Providers. Defendants exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the devices by placing the Session Replay Code to stalk users of their websites.

465. As to the data, Defendants used Plaintiffs' and Class Members' data by transferring it from Plaintiffs' device Plaintiffs' data to the Cloud Storage Data Centers of the Session Replay Providers for the purpose of using the data to make money without paying for the valuable data. Defendants exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data by capturing, taking, and/or using the data without permission or consent from Plaintiffs and the Classes.

466. Plaintiffs' data that was transferred from Plaintiffs' and Class Members' respective devices are maintained in cloud storage devices located on servers across the nation.

467. As noted and for example, Clarity data is stored in the Microsoft Azure cloud

service.[49] The Azure Cloud Data Center locations (which host their services) are located across the United States and elsewhere.[50]

468. Microsoft provides the following only regarding the Azure cloud service it offers to Session Replay Providers:

> As a customer, you *maintain ownership of customer data*—the content, personal and other data you provide for storing and hosting in Azure services. You are also in control of any additional geographies where you decide to deploy your solutions or replicate your data.[51]

469. Quantum Metric stores data on the Google Cloud Platform.[52] Google Cloud is located in 9 locations in the US alone.[53] Google represents:

> Rather than storing each user's data on a single machine or set of machines, we distribute all data — including our own — across many computers in different locations.[54]

470. As such, Plaintiffs' and Class Members' data is tied to something tangible – i.e., Microsoft and/or Google Servers.

471. All Session Replay Providers operate in a similar manner with cloud devices and servers.

472. As set forth above, Defendants exercised dominion and ownership over Plaintiffs' and Class Members' personalty inconsistent with, and in denial of, the rights of Plaintiffs' and the Classes.

473. Plaintiffs and the Classes did not consent to the aforementioned interference.

[49] *See supra* note 43.

[50] *See supra* note 44.

[51] *See supra* note 45.

[52] *See supra* note 46.

[53] *See supra* note 47.

[54] *See supra* note 48.

474. The aforementioned interference was the actual and proximate cause of injury to Plaintiffs and the Classes because it exposed their respective private data and/or personally identifiable information and/or other data to one or more third parties.

475. Additionally, the interference gave third parties the data and information without the consent of Plaintiffs and the Classes, and which is valuable, and for which Defendants did not obtain informed consent nor pay Plaintiff or the Classes to obtain.

476. Plaintiffs and the Classes are entitled to recover the actual damages they suffered as a result of Defendants' aforementioned interference with their respective devices and/or data in an amount to be determined at trial.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of the other members of the proposed Classes, respectfully request that the Court enter judgment in Plaintiffs' and Class Members' favor and against Defendants as follows:

A. Certifying the Nationwide Class and State Subclasses and appointing Plaintiffs as the representatives of the Classes;

B. Appointing Plaintiffs' counsel as class counsel;

C. Declaring that Defendants' past conduct was unlawful, as alleged herein;

D. Declaring Defendants' ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendants from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiffs, the Nationwide Class, and State Subclass Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiffs, the Nationwide Class Members, and State Subclass Members pre-judgment and post-judgment interest;

H. Awarding Plaintiffs, the Nationwide Class Members, and State Subclass Members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Classes, demand a trial by jury of any and all issues in this action so triable of right.

Date: August 14, 2023

By: */s/ Kate M. Baxter-Kauf*
Kate M. Baxter-Kauf
Karen Hanson Riebel
Maureen Kane Berg
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

Nicholas A. Colella (PA Bar # 332699)
Gary F. Lynch (PA Bar # 56887)
Kelly K. Iverson (PA Bar # 307175)
Jamisen Etzel (PA Bar # 311514)
Elizabeth Pollock-Avery (PA Bar # 314841)
Patrick Donathen (PA Bar # 330416)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
NickC@lcllp.com
Gary@lcllp.com
Kelly@lcllp.com
Jamisen@lcllp.com
Elizabeth@lcllp.com
Patrick@lcllp.com

Katrina Carroll
LYNCH CARPENTER, LLP
111 W. Washington St. Suite 1240
Chicago IL 60602
Tel: (312) 750-1265
katrina@lcllp.com

Joseph H. Kanee
MARCUS & ZELMAN LLC
701 Brickell Avenue, Suite 1550
Miami, FL 33131
Tel: (786) 369-1122
joseph@marcuszelman.com

Ari H. Marcus (PA Bar # 322283)
MARCUS & ZELMAN LLC
701 Cookman Avenue, Suite 300

Asbury Park, NJ 07712
Tel: (732) 695-3282
ari@marcuszelman.com
Plaintiffs' Co-Lead and Liaison Counsel

Carey Alexander
SCOTT & SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue
Ste 17th Floor
New York, NY 10169
Tel: (212) 223-6444
calexander@scott-scott.com

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Tel: (404) 978-6971
mgibson@thefinleyfirm.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street Fourteenth Floor
New York, NY 10004
Tel: (646) 357-1100
snathan@hausfeld.com

James J. Pizzirusso (Md. Bar No. 20817)
HAUSFELD LLP
888 16th Street N.W. Suite 300 Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com
Plaintiffs' Steering Committee